UNIVERSITE LIBANAISE (Faculté de Génie)

UNIVERSITE SAINT-JOSEPH (Faculté d'Ingénierie)

Sous l'égide de l'Agence Universitaire de la Francophonie
AUF

Diplôme d'Etudes Approfondies
Réseaux de télécommunications

La sécurisation de la téléphonie sur IP

Par

Marguerite Fayçal

Encadré par : **M. Nicolas Rouhana**

Soutenance le 20 décembre 2004 devant le jury composé de

MM.	Samir Tohmé	Président
	Mohamad Zoaeter	Membre
	Wajdi Najem	Membre
	Imad Mougharbel	Membre
	Nicolas Rouhana	Membre
	Mahmoud Doughan	Membre
	Maroun Chamoun	Membre

Je remercie M. Nicolas ROUHANA pour tous les efforts, directives et encadrements qu'il a entrepris et déployés pour m'aider à la réalisation de ce projet. M. ROUHANA m'a comblée de sa patience et de sa complaisance souriantes.

Je tiens aussi à exprimer ma gratitude à M. Ahmed SERHROUCHNI pour ses directives explicatives, claires, concises et précises. L'érudition accueillante de M. SERHROUCHNI a bien servi mes efforts et orientations.

Un grand merci à Carole BASSIL pour son amitié, sa gentillesse et ses services rendus qui ont contribué à me donner un souffle nouveau pour parfaire certaines parties de ce mémoire.

Enfin, je ne pourrais terminer sans exprimer toute ma reconnaissance à mon père pour son soutien, son enthousiasme, ses encouragements et ses précieux conseils, et ma gratitude affectueuse à ma mère et à ma sœur pour leur patience, présence et entrain qui m'ont si bien accompagnée à suivre les jalons du chemin jusqu'à la ligne d'arrivée de la soutenance finale et son heureux aboutissement.

TABLE DES MATIÈRES

SUJET

Sujet N°12 : Sécurisation de la téléphonie sur IP

La dérégulation des télécommunications et l'avancée des technologies IP accentuent la nécessité de la sécurisation de la téléphonie d'une manière générale et encore plus la téléphonie sur IP. Les techniques et architectures de la téléphonie sur IP sont maintenant bien établies en termes : de standardisation, de protocoles (H.323, QoS,...) et d'équipements. La phase suivante à atteindre reste celle de la sécurisation de ce service.

Les solutions de sécurité classiques ne répondent pas aux exigences de la sécurité de la téléphonie sur IP. Il est ainsi nécessaire de définir des mécanismes et protocoles spécifiques et les intégrer aux architectures existantes.

Plusieurs programmes de recherche mondiaux ont été lancés pour atteindre cet objectif. Plusieurs directions de l'armement de plusieurs pays soutiennent des programmes de recherche sur plusieurs années. Cette valeur ajoutée pour l'industrie est critique pour définir les nombreuses applications et autres services à mettre en œuvre, à l'usage de l'utilisateur final et des acteurs économiques.

Un effort important a été ainsi investi par la NSA (National Security Agency) pour définir une architecture de bout en bout pour la sécurisation de la téléphonie.

Cette architecture de signalisation se veut indépendante de tout type d'infrastructure et peut ainsi être basée sur des réseaux fixes ou mobiles ou des réseaux de données tels que IP.

Toute la documentation vous sera fournie pour atteindre les résultats spécifiés dans les objectifs ci-dessous.

Travail :

Les objectifs à atteindre pour ce travail sont dans un premier temps d'étudier et d'analyser l'architecture et les protocoles proposés par la NSA et dans un second d'étudier l'impact de cette architecture sur les infrastructures de la téléphonie existantes

Ensuite, il est demandé l'intégration des protocoles de signalisation pour la sécurisation de la téléphonie proposés par la NSA dans l'architecture H323.

SOMMAIRE

Depuis l'invention du premier téléphone par Alexandre Graham Bell en 1869, la téléphonie n'a cessé d'évoluer : de la commutation de circuit à la commutation par paquet, pour passer ensuite à la voix sur IP, au GSM, à la voix sur IP sur réseau mobile. Aujourd'hui, en 2004, la téléphonie vit l'une des périodes les plus critiques de son évolution technologique.

Au début des années 80, la transmission sécurisée de la voix était réalisée avec des solutions propriétaires au sein du réseau fixe traditionnel. Les utilisateurs devaient posséder des terminaux compatibles pour échanger l'information de voix de façon sécurisée entre deux dispositifs issus du même fabricant. Lors de l'essai de l'établissement d'une communication sécurisée entre dispositifs de fabricants différents, la sécurité a été compromise.

Dans les années 90, l'interopérabilité des communications de voix traditionnelles sécurisées a été réalisée par le développement d'un matériel de communications interopérables basé sur des standards de sécurité. Des dispositifs de fabricants différents configurés avec ce nouveau standard ont pu alors communiquer de façon sécurisée.

Un intérêt grandissant s'est fait ressentir ces dernières années pour l'intégration de la téléphonie avec l'informatique. Aujourd'hui, les flux téléphoniques, signalisation et communications elles-mêmes, se mettent à emprunter des réseaux informatiques… Un seul réseau est utilisé pour le transport de la voix et des données. On parle de la « téléphonie sur IP », qui fait l'objet du premier chapitre de ce rapport : sa définition, ce qui la diffère de la « voix sur IP », leurs caractéristiques communes, les éléments clés d'une communication de téléphonie sur IP,…

De nombreux avantages, comme celui de la simplicité de l'administration ou la baisse des coûts de déploiement (dans certains cas) justifient que l'on s'intéresse à cette technologie, mais pas suffisamment, tant que se posent certains problèmes, pas encore résolus, notamment en matière de sécurité.

En effet, la nature des réseaux ouverts a un impact sur la voix en terme de sécurité, d'où le besoin imminent de sécuriser la voix tout en assurant une bonne qualité de service à la voix et aux données, aussi bien dans un réseau fixe que dans un réseau mobile.

Les développements en matière des technologies de communications (RNIS, CDM, TDM, IP, ATM, etc.) ont fragmenté le réseau téléphonique suivant les multiples technologies déployées, ce qui a mené à des solutions qui ne sont pas interopérables. Avec plus d'une architecture, les utilisateurs ne pouvaient pas communiquer de façon sécurisée. En plus, la déréglementation a résulté en de multiples compagnies de réseau dans un même secteur, ce qui a empiré le problème comme si la force d'unification jadis fournie par le système Bell n'existait plus.

D'où l'intérêt de faire du deuxième chapitre une analyse critique de la téléphonie sur IP et d'aborder ses avantages, ses faiblesses, les motivations tant techniques qu'économiques, qui nous poussent à sécuriser la voix, ainsi que l'état de l'art actuel et l'avenir perspectif de la ToIP.

Tout comme des solutions de sécurisation sont proposées pour les données, chaque opérateur a fourni des efforts pour sécuriser les transmissions de voix. Mais ces mécanismes propriétaires rendent impossible l'interopérabilité sécurisée entre les différentes plateformes. En général, la sécurité de la VoIP exige beaucoup plus d'interventions étendues pour réaliser le même niveau de base de la sécurité qui a été assumé avec le système traditionnel, surtout parce que le risque s'est déplacé d'un accès physique à un accès virtuel.

Plusieurs architectures ont été créées où la voix est combinée aux données et à l'imagerie. Deux normes principales sont utilisées pour transporter l'information de voix sur des réseaux IP : SIP, un protocole de l'IETF et H.323, une famille protocolaire de l'ITU-T, qui regroupe une diversité de protocoles nécessaires à la voix, aux données et à l'imagerie, à la signalisation et au contrôle et qui fait l'objet du troisième chapitre.

SIP et H.323 sont tous deux vulnérables aux attaques puisque beaucoup d'aspects de ces systèmes sont susceptibles d'offrir un terrain fertile à ceux intéressés d'exploiter VoIP. Beaucoup de normes sont utilisées pour sécuriser les communications de VoIP, telles que H.235 qui définit la sécurité pour H.323. SIP se sert de mécanismes d'authentification semblables à HTTP alors qu'il utilise PGP pour les services d'intégrité et de confidentialité.

Pour la sécurisation de la voix indépendamment de l'opérateur, des solutions partielles voire incomplètes sont déjà proposées. L'information de voix transportée dans des paquets RTP pourrait être sécurisée avec le protocole SRTP (*Secure RTP*). L'ensemble des services de sécurité dans IPSec est fourni à la couche IP, offrant une protection pour IP et/ou les protocoles de couche supérieure. Ainsi, IPSec peut être utilisé pour protéger le trafic de signalisation de VoIP (c.-à-d., SIP et H.323) et le trafic des utilisateurs de VoIP (c.-à-d. RTP). Tous ces mécanismes peuvent être utilisés pour sécuriser des communications de voix sur des réseaux basés sur IP mais ne pourraient pas être étendus à d'autres réseaux, non basés sur IP. Le quatrième chapitre expose alors les architectures candidates et les solutions perspectives pour la sécurisation de la voix.

Récemment, un nouveau protocole de sécurité, le Future Narrow Band Digital Terminal a été présenté par la National Security Agency. Le but premier de FNBDT, quand il a été créé, était de réaliser des communications sécurisées universellement interopérables sur les réseaux à fil et les réseaux sans fil, sur les réseaux actuels et les réseaux émergents, etc. FNBDT est donc un protocole de signalisation sécurisée de bout-en-bout qui permettra l'établissement de communications interopérables et sécurisées entre des dispositifs qui ne sont pas configurés pour communiquer ensemble de manière sécurisée. Il n'est dépendant d'aucun réseau spécifique. Pour assurer l'interopérabilité entre différentes plateformes, l'abstraction des couches physique et réseau doit être fournie avec une transparence de l'utilisateur.

Le cinquième chapitre de ce rapport est consacré à FNBDT et mon travail se base sur la spécification 1.1 de la signalisation FNBDT ; une nouvelle version pouvant apporter des modifications ou des améliorations.

Le sixième et dernier chapitre commence par une analyse critique du protocole FNBDT, suivie d'une comparaison de ses mécanismes de sécurité avec celles offertes par SRTP, en référence à celles offertes par H.235. Il se poursuit par une étude comparative de FNBDT et SRTP, à des niveaux autres que la sécurité et se termine par une proposition d'intégration de FNBDT à H.323.

Ce rapport, au long duquel je préférerai les termes anglo-saxons par souci de commodité, se termine par une conclusion et une ouverture sur des perspectives futures.

CHAPITRE 1

LA TELEPHONIE SUR IP

1.1 - Que faut-il penser de la téléphonie sur IP ?

1.1.1 - Qu'est-ce que la téléphonie sur IP ?

Depuis les années quatre-vingt, les éditeurs de logiciels cherchent à utiliser le réseau informatique pour y véhiculer de la voix. Suite à l'apparition de protocoles comme H.323 ou SIP, les constructeurs d'autocommutateurs ont progressivement intégré cette dimension IP à leurs solutions dans une optique de convergence voix-données. Dans un premier temps, cette convergence a pris la forme de cartes optionnelles à intégrer dans les PABX (« *Private Automatic Branch eXchange* ») existants, pour être proposée aujourd'hui de façon native. C'est ce qu'on appelle la Téléphonie sur IP (« *Telephony over IP* » ou ToIP).

La ToIP consiste donc en un ensemble de techniques qui, dans une entreprise ou un organisme, permettent la mise en place des services téléphoniques sur un réseau IP en utilisant la technique de la Voix sur IP (« *Voice over IP* » ou VoIP) pour la transmission de messages vocaux sur des réseaux de données à paquets utilisant le protocole IP.

ToIP est de fait la première alternative réelle aux réseaux traditionnels de téléphonie qui utilisent une technologie dite de commutation de circuits (*voice switching*) vieille de plus de 100 ans.

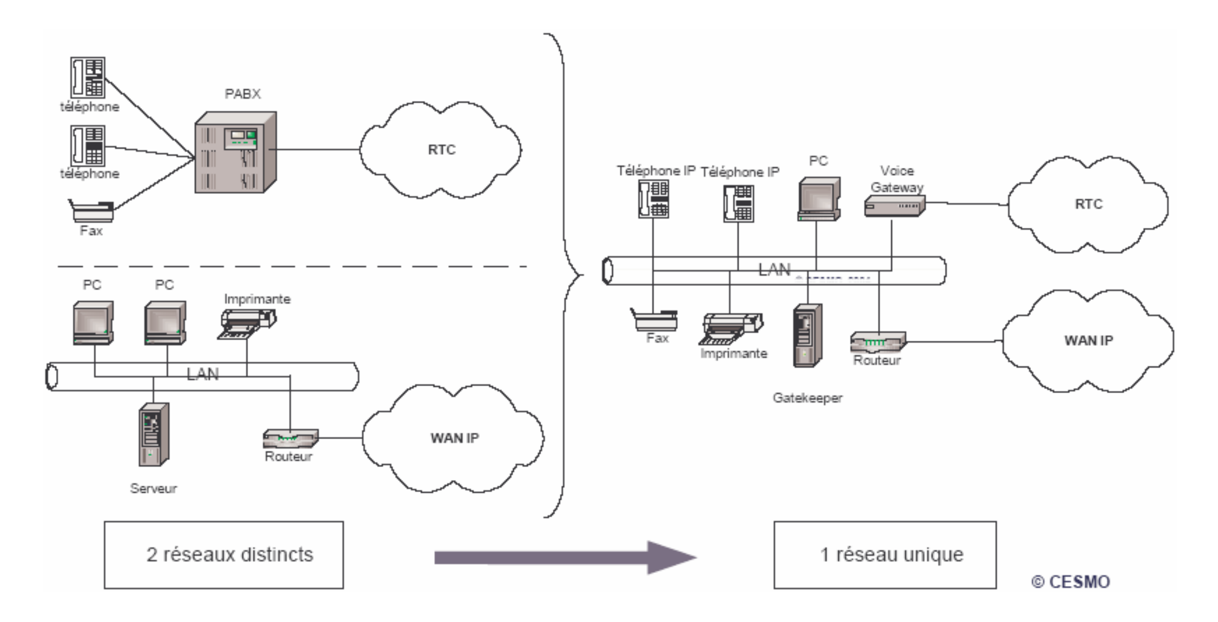


Figure 1.1 : *Schéma de convergence des réseaux.*

ToIP n'est pas de la téléphonie sur Internet, malgré une confusion souvent entretenue dans les médias.

Le terme « Téléphonie sur Internet » est spécifiquement utilisé lorsqu'on se sert du grand réseau public Internet pour établir des communications téléphoniques. L'Internet que nous utilisons tous les jours est un réseau de réseaux qu'aucune organisation ne contrôle ou ne gère dans son ensemble. Il n'y pas de garantie de qualité de service.

Au contraire, la téléphonie sur IP est confiée à un réseau géré par une entité unique, une entreprise pour ses besoins internes ou un opérateur télécom. La différence en terme de qualité de service est énorme or, la voix est très sensible à tout retard dans la diffusion du signal. C'est ainsi que nous avons souffert de la piètre qualité des appels téléphoniques transatlantiques transmis par satellite car le temps de retour du signal depuis le satellite produisait un écho nuisible à la qualité de la conversation.

Pour être exhaustif, mentionnons le fait qu'il était déjà possible de faire passer de la voix sur des réseaux de données à paquets tels que Frame Relay (« *Voice over Frame Relay* » ou VoFR) ou ATM (« *Voice over ATM* » ou VoATM), ce qui permet de garantir la transmission de bout en bout de l'intégralité des paquets et qui plus est dans l'ordre d'émission. Mais pour autant, ces dernières technologies n'ont jamais atteint une échelle vraiment significative.

1.1.2 - Téléphonie sur IP, ou Voix sur IP ?

Avant d'entrer dans les détails des différents atouts de la ToIP, il est nécessaire de la distinguer de la VoIP. Dans les deux cas, nous parlons d'équipements et de mécanismes permettant de transporter de la voix sur un réseau de données de type IP (*Internet Protoco*l).

Dans le cas de la VoIP, on se contente d'interconnecter des PABXs en capsulant la voix numérisée, dans les paquets IP. Ces derniers sont ensuite véhiculés au sein du réseau de données, de manière classique, comme des paquets de données. La voix est simplement « reconstituée » lorsque les paquets arrivent chez le destinataire. Un exemple « parlant » de VoIP se trouve dans le raccordement de 2 sites via une ligne spécialisée qui transporte la voix et les données.

Quant à la ToIP, elle va plus loin que la VoIP en terme de mécanismes et d'équipement, cherchant à apporter aux utilisateurs la qualité de service (qualité de transmission, qualité de voix, disponibilité du service) et les services que ces derniers sont l'habitude de trouver du côté de la téléphonie classique (présentation du numéro, transfert d'appel, conférence, etc.) le tout sans faire appel aux PABXs.

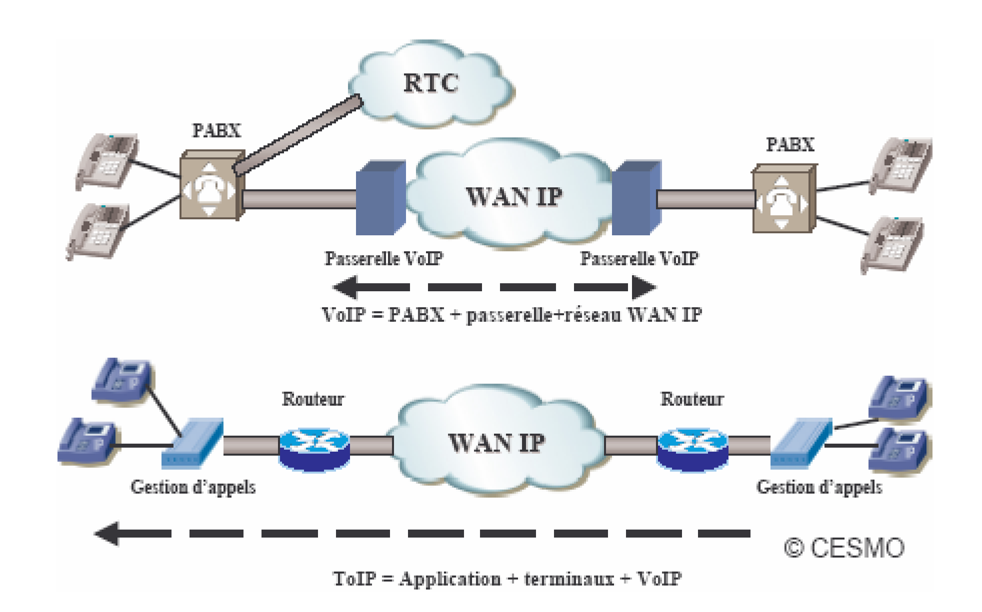


Figure 1.2 : *Périmètres comparés de la VoIP et de la ToIP.*

La VoIP est donc une composante de la ToIP et sa sécurisation est, par conséquent, la condition sine qua non de la sécurisation de la ToIP.

Similairement au cas de la téléphonie, il faut distinguer la voix sur IP de la voix sur Internet, dépendamment du réseau IP utilisé pour le transport des paquets de la voix : s'il s'agit d'un réseau IP privé ou du réseau des réseaux, l'Internet.

Il est aussi à noter que dans le cadre de la téléphonie sur IP, l'on distingue la téléphonie *fixe* sur IP et la téléphonie *mobile* sur IP. Cependant, je me limiterai dans le cadre de ce rapport à la téléphonie *fixe* sur IP, que je désignerai tout court par ToIP, sauf indication explicite contraire.

1.2 - La Voix sur IP

1.2.1 - Les caractéristiques de la voix

Le système vocal est complexe et basé sur des ondes sonores de fréquences différentes. Le spectre des fréquences perçues par l'oreille humaine s'étale de 100 Hz à 20 kHz. Cette fourchette est, cependant, à réduire si l'on veut distinguer les fréquences utiles des fréquences audibles. En effet, la quasi-totalité d'un message sonore est compréhensible dans la fourchette 300-3400 Hz. Cette dernière correspond, d'ailleurs, à celle utilisée par le téléphone standard.

Une conversation entre deux personnes respecte deux principes : intelligibilité et interactivité. Couper la parole à quelqu'un ne se fait pas, mais c'est un gage d'interactivité et de dialogue. En terme de transmission numérique, cela se traduit par le terme duplex. Une conversation full duplex assure cette interactivité car chaque locuteur peut parler en même temps, ce qui arrive quand deux personnes parlent de leur propre expérience sans s'écouter... Un mode half duplex induit une conversation unidirectionnelle du style CB (« Citizen Band ») :

« quel est ton QRZ, à toi ! je viens de Moselle, à toi ! »

Cette interactivité implique des notions de délais dans le transport de la voix (avec le téléphone, par exemple). Le délai maximum acceptable pour une transmission optimale de la voix [ITU G.114] est de 150ms pour les communications sur voies bifilaires et 250 à 300 ms pour les communications satellitaires. Jusqu'à 400 ms (limite supérieure) le dialogue reste tout de même assez réactif. Au-delà de cette limite le contradicteur aura l'impression de parler dans le vide.

1.2.2 - Transmission de la voix en mode paquet

La téléphonie sur IP est une transmission de la voix en mode paquets. Le concept de la VoIP, une technologie récente et datant de 1996, est en théorie plutôt séduisant : fusionner les infrastructures télécoms et réseaux sur un même câblage.

Pour acheminer la voix à travers le réseau IP, il faut réduire au maximum le signal vocal en lui apportant le moins de dégradations possibles car le débit nominal de transport de la voix codée MIC (Modulation par Impulsions et Codage) à travers le RTC (Réseau Téléphonique Commuté) est de 64 kbps alors que la bande passante nominale pour un réseau IP est nettement inférieure à 64 kbps (14.4, 28.8, 56 kbps).

Pour comprendre le traitement complexe de la voix analogique (signaux électriques) en signaux binaires, voici un synoptique explicatif :

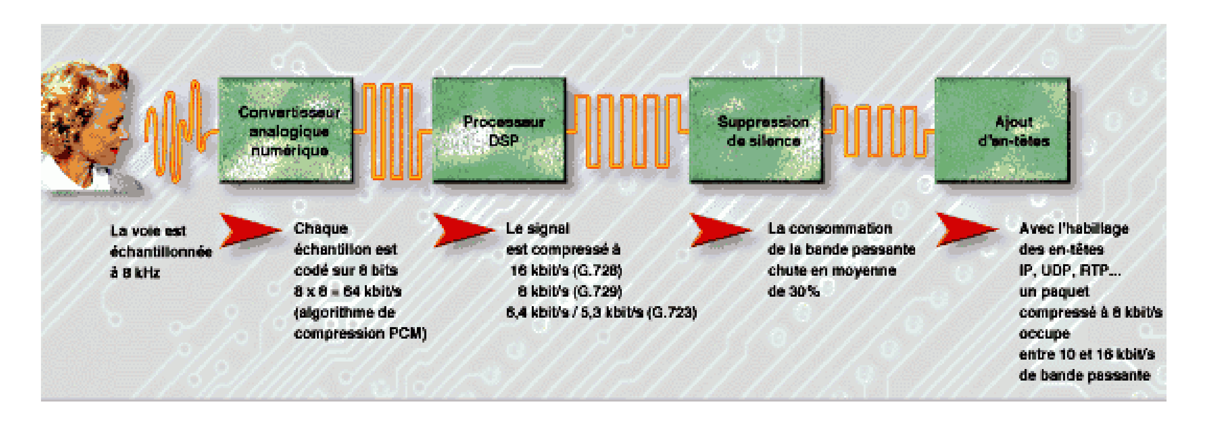


***Figure 1.3 :** Synoptique de transmission de la voix analogique en mode paquet.*

Explications du synoptique : la bande voix qui est un signal électrique analogique utilisant une bande de fréquence de 300 à 3400 Hz, est d'abord échantillonnée numériquement par un convertisseur et codée sur 8 bits. Par la suite, elle est compressée par les fameux codecs (il s'agit de processeurs DSP) selon une certaine norme de compression variable selon les codecs utilisés, et ensuite on peut éventuellement supprimer les pauses de silences observés lors d'une conversation, pour ensuite ajouter les en-têtes RTP,UDP et enfin IP. Une fois que la voix est transformée en paquets IP, ces petits paquets IP identifiés et numérotés peuvent transiter sur n'importe quel réseau IP (ADSL, Ethernet, Satellite,routeurs, switchs, PC, Wifi, etc...)

A l'arrivée, les paquets transmis sont ré-assemblés et le signal de données ainsi obtenu est décompressé puis converti en signal analogique pour restitution sonore à l'utilisateur.

1.2.3 - Les différents codecs et taux de compression

Les codecs sont des chipsets qui font office de compresseurs/décompresseurs ou de codeurs/décodeurs. Certains terminaux IP-PHONES n'acceptent qu'une partie ou même un seul codec, tout dépend du modèle de terminal et du constructeur. Le principe de fonctionnement de ces codecs est expliqué par le synoptique de transmission de la voix en mode paquet. Les principaux taux de compression de la voix sont les codecs officiels suivants :

CoDec	Débit binaire (Kbps)	Délai de codage (ms)	MOS ou Qualité auditive perçue
G.711 PCM	64	0,125	4,1
G.726 ADPCM	32	0,125	3,85
G.728 LD-CELP	15	0,125	3,61
G.729 CS-ACELP	8	10	3,92
G.729a CS-ACELP	8	10	3,7
G.723.1 MP-MLQ	6,3	30	3,9
G.723.1 ACELP	5,3	30	3,65

Tableau 1.1 : *Comparatif des caractéristiques des CoDecs ITU-T courants.*

Le MOS (« *Mean Opinion Score* ») est le score d'opinion moyen. C'est une mesure utilisée pour évaluer la qualité de la voix restituée par un système de téléphonie, incluant l'ensemble des contraintes de codage, compression et transport. Elle est le résultat de la notation de différents signaux voix réalisée par un groupe d'écouteurs sur une échelle de 1 à 5 (1=mauvais, 2=médiocre, 3=moyen assez bon, 4=bon, 5=excellent). Des analyseurs de QoS ToIP peuvent également mesurer ce score MOS.

1.2.4 - Les contraintes de la VoIP

Le transfert de la voix sur un réseau IP est un chemin semé d'embûches. Il est donc nécessaire d'expliquer comment arrivent ses défauts de transmission. Les trois principales causes des difficultés et des limites associées à VoIP sont : le délai de latence, la gigue et le taux de perte des paquets.

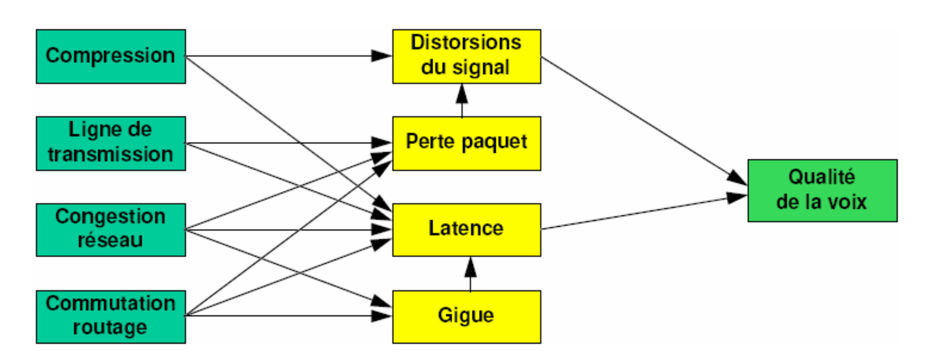


Figure 1.4 : *Les contraintes de la VoIP.*

1.2.4.1 - Le délai de latence

Pour une application voix sur IP, plusieurs facteurs influencent le délai durant une transmission. Sur le chemin que prendrait une transmission de voix, après la numérisation du signal, un délai minimal de 150 ms est introduit par :

– le codage du signal par le CODEC (0.75 ms – 30 ms) [ITU G.729, G.723, etc.] ;
– la compression ;
– la mise en paquet ;
– le passage en file d'attente d'émission ;
– la propagation dans le réseau (délai de traitement dans les routeurs qui peut atteindre les 30 ms) ;
– la bufférisation en réception (l'arrivée des paquets dans des tampons, afin d'être livrés à un débit uniforme, cause une variation de délai (gigue) de 40 ms à 70 ms) ;
– la dépaquetisation ;
– la décompression ;
– le décodage ;
– et la restitution (conversion numérique analogique).

Il est aussi à noter que les délais d'acheminement du signal vocal sont d'autant plus importants que les délais dus à l'écho le sont. L'écho c'est le délai entre l'émission du signal et la réception de ce même signal en réverbération. Cette réverbération est causée par les composants électroniques des parties analogiques. L'annulation des échos électrique et acoustique se fait par des annulateurs d'échos électriques EEC (« *Electrical Echo Cancellers* ») et des annulateurs d'échos acoustiques AEC (« *Acoustic Echo Cancellers* »). Tant que l'écho est inférieur à 50 ms, il n'est pas perceptible. Plus il est décalé dans le temps, plus il est insupportable.

Quantifier le délai de transmission sur le réseau de manière fiable est donc quasi impossible, car il y a trop d'inconnues. Cependant, la valeur optimale couramment admise en VoIP, pour le délai d'un aller simple, est inférieure ou égale à 100 ms et ce délai reste acceptable jusqu'à une valeur de 200ms afin de respecter les contraintes d'une conversation interactive.

1.2.4.2 - La gigue (ou « Jitter »)

La gigue, c'est la variation des écarts de délais de transmission entre des paquets consécutifs. Elle nécessite la mise en place de buffers en réception qui lissent ces écarts pour retrouver le rythme de l'émission, ce qui a pour effet néfaste d'augmenter le délai de transmission.

La valeur optimale couramment admise en VoIP, pour la gigue, est inférieure ou égale à 40 ms et la valeur acceptable est inférieure ou égale à 75ms.

1.2.4.3 - Le taux de perte des paquets

La perte d'un paquet fait partie intégrante du concept de transmission IP. Elle entraîne la disparition d'un ou plusieurs échantillons du flux voix, on parle alors de *distorsions du signal*. Suivant le nombre de paquets perdus, la qualité sonore en bout de ligne peut s'en ressentir. Des solutions de retransmission des paquets de voix engendreraient des délais trop importants. Si les paquets perdus ne le sont pas en rafales, les codecs sont capables de « reconstruire » via des algorithmes prédictifs les échantillons manquants, du moins jusqu'à un certain seuil. Ce seuil est traduit en taux de pertes.

La valeur optimale du taux de perte, couramment admise pour un service de VoIP, est inférieure ou égale à 1% et la valeur acceptable est inférieure ou égale à 3%.

1.3 - Caractéristiques de la ToIP

Depuis son invention par A. Graham Bell, le premier téléphone possédait déjà les fonctionnalités de signalisation par les états décroché/raccroché et la composition du numéro d'abonné distant, ainsi que par les facilités d'envoyer les signaux vocaux de la conversation sur le lien bifilaire. La téléphonie est donc composée de deux plans, un plan usager par lequel circulent les échantillons de voix en provenance de l'écouteur du poste téléphonique et le plan contrôle où s'effectuent l'échange de la signalisation pour l'établissement et la terminaison de l'appel.

Avec la numérisation des centraux téléphoniques et l'introduction du réseau numérique à intégration téléphonique, il y a eu séparation du plan de l'usager du plan de contrôle. Les messages de signalisation sont donc commutés dans un commutateur de paquet et les informations de voix sont échangées dans un réseau à commutation de circuit. Avec l'évolution des technologies, on est passé vers une transmission sans fil dans les réseaux mobiles et donc vers un monde plus vulnérable aux attaques et aux fraudes sur les liaisons radios. La notion de signalisation de l'appel et d'échanges des informations de voix existent toujours même en passant à la voix sur IP.

Par ailleurs, toutes les contraintes de la VoIP (cf. paragraphe 1.2.4) sont inhérentes à la ToIP et les contraintes et défauts inhérents à IP sont les fondements des difficultés rencontrées par le concept VoIP. Or, le transport de la ToIP ne doit souffrir d'aucun retard de transmission, ni d'altérations (attention aux firewalls), ni de perte de paquets. Due à ces contraintes temporelles, la taille des paquets de voix se limitera entre 10 et 50 bytes de données utiles.

De plus, les applications temps réel – i.e., la vidéoconférence, Voix sur IP, vidéo temps réel – imposent des contraintes temporelles, présentent certaines vulnérabilités au niveau de la transmission des paquets et posent des problèmes de synchronisation temporelle.

La sécurité est donc aussi bien nécessaire aux informations de voix qu'aux informations de signalisation nécessaires à l'établissement de l'appel et aux services, qui transportent des informations critiques comme l'identifiant du numéro appelé et appelant, etc. Or, introduire une nouvelle couche de sécurité, garantissant la confidentialité, l'intégrité et l'authentification, ralentit la transmission des paquets et augmente le délai…

1.4 - Les équipements clés d'une communication ToIP

Les principaux équipements d'une communication IP sont : les terminaux téléphoniques IP, le « *gatekeeper* » et la « *voice gateway* ».

1.4.1 - Les terminaux téléphoniques

1.4.1.1 - Le « hardphone » IP

L'« *IP-phone* » ou « *hardphone* » est un terminal téléphonique totalement indépendant de l'équipement informatique, destiné à remplacer l'équipement de téléphonie classique existant et, fonctionnant sur le réseau LAN IP à 10/100 avec une norme soit propriétaire, soit SIP, soit H.323. Il peut y avoir plusieurs codecs (G.711 obligatoire) pour l'audio, et il peut disposer d'un écran monochrome ou couleur, et d'une ou plusieurs touches soit programmables, soit préprogrammées. Il est en général doté d'un hub passif à un seul port pour pouvoir alimenter le PC de l'utilisateur (l'IP-phone se raccorde sur la seul prise Ethernet mural et le PC se raccorde derrière l'IP-phone).



Figure 1.5 : *Modèles de « hardphone » IP.*

1.4.1.2 - Le « softphone » IP

Le « *softphone* » est un logiciel qui assure toutes les fonctions téléphoniques et qui utilise la carte son et le micro du PC de l'utilisateur, et aussi la carte Ethernet du PC. Il est géré soit par le Call Manager, soit par le PABX-IP.



Figure 1.6 *: Modèles de « softphone » IP.*

1.4.1.3 - L'alimentation des postes IP

Un poste IP (ou « *IP-phone* ») a besoin d'une alimentation :

- soit *locale* : le poste dispose alors d'une alimentation externe DC de 48Volts, ce qui nécessite l'utilisation d'un petit transformateur 220V~/48VDC pouvant être facilement oublié et débranché avec une fausse manipulation ;
- soit *distante* : le poste est alors télé-alimenté :
  - soit par le commutateur Ethernet selon la norme 802.3af de IEEE Computer Society ;
  - soit par un équipement intermédiaire appelé MID-SPAN, situé entre le switch et le panneau de câblage.

Il est à noter qu'en cas de panne secteur, il n'y a plus de téléphone (c'est normal) et aucun appel d'urgences n'est donc possible.

1.4.2 - Les « gatekeeper »

Le « *gatekeeper* », ou garde-barrière, effectue les translations d'adresses (identifiant H.323 ou SIP et adresse IP du référencement du terminal) et gère la bande passante et les droits d'accès. C'est le point de passage obligé pour tous les équipements de sa zone d'action.

Physiquement, un « *gatekeeper* » est un serveur informatique localisé sur le même réseau que les terminaux téléphoniques IP.

1.4.3 - Les « voice gateway »

Le « *voice gateway* », ou passerelle, est un élément de routage équipé de cartes d'interfaces analogiques et/ou numériques pour s'interconnecter avec soit d'autres PABX (en QSIG, RNIS ou E&M), soit des opérateurs de télécommunications locaux, nationaux ou internationaux. Plusieurs passerelles peuvent faire partie d'un seul et même réseau, ou l'on peut également avoir une passerelle par réseau local (LAN). La passerelle peut également assurer l'interface de postes analogiques classiques qui pourront utiliser toutes les ressources du réseau téléphonique IP (appels internes et externes, entrants et sortants).

1.4.4 - Les équipements complémentaires

D'autres équipements peuvent entrer aussi dans la composition des réseaux de ToIP :

- le *PABX-IP*, c'est lui qui assure la commutation des appels et leurs autorisations, il peut servir aussi de routeur ou de switch dans certains modèles, ainsi que de serveur DHCP. Il peut posséder des interfaces de type analogiques (fax), numériques (postes), numériques (RNIS, QSIG) ou opérateurs (RTC-PSTN ou EURO-RNIS). Il peut se gérer par IP en intranet ou par un logiciel serveur spécialisé que ce soit en interne ou depuis l'extérieur. Il peut s'interconnecter avec d'autres PABX-IP ou PABX non IP de la même marque (réseau homogène) ou d'autres PABX d'autres marques (réseau hétérogène) ;
- le *serveur de communications*, il gère les autorisations d'appels entre les terminaux IP ou « *softphones* » et les différentes signalisations du réseau. Il peut posséder des interfaces réseaux opérateurs (RTC-PSTN ou RNIS), sinon les appels externes passeront par la passerelle dédiée à cela (*gateway*) ;
- le *MCU* (« *Multipoint Control Unit* ») est un élément optionnel et gère les conférences audio vidéo.

Enfin, outre ces fonctionnalités basiques, les systèmes de ToIP savent proposer des fonctions de péritéléphonie à travers les équipements suivants :

- plate-forme de supervision et d'administration ;
- serveurs de messagerie vocale ;
- standards téléphoniques ;
- serveurs de taxation ;
- serveurs d'enregistrement.

1.5 - Les différents protocoles utilisés

Il existe plusieurs approches pour offrir des services de téléphonie et de visiophonie sur des réseaux IP. Certaines placent l'intelligence dans le réseau alors que d'autres préfèrent une approche pair-à-pair avec l'intelligence répartie à la périphérie (terminal de téléphonie IP, passerelle avec le réseau téléphonique commuté...). Chacune a ses avantages et ses inconvénients, et ces diverses approches se déclinent au travers de différents protocoles.

Dans ce paragraphe, je me limiterai à un court descriptif des 3 protocoles non propriétaires utilisés pour la VoIP, à savoir :

- le protocole H.323 ;
- le protocole SIP ;
- les protocoles pour terminaux simples : MCGP/MEGACO.

1.5.1 - Le protocole H.323

En 1996 naquît la première version voix sur IP appelée H323. Issu de l'organisation de standardisation européenne ITU-T sur la base des travaux de la série H.320 sur la visioconférence sur RNIS (signalisation voix Q.931), ce standard a été développé pour les centraux téléphoniques sur la base de PBX et a maintenant donné suite à de nombreuses évolutions, quelques nouveaux standards prenant d'autres orientations technologiques. En réalité, H.323 est une famille de protocoles constituant déjà une norme stabilisée ayant de nombreux produits sur le marché (terminaux, gatekeeper, gateway, logiciels) et existe actuellement en cinq versions (v.1 à v.5).

Une étude détaillée de cette famille protocolaire fait l'objet du chapitre 3.

1.5.2 - Le protocole SIP

En 1997, l'IETF conçoit un système de signalisation SIP (« *Session Initiation Protocol* ») adapté à la philosophie IP, contrairement à H.323 qui s'inspire des circuits télécoms. SIP se base en premier lieu sur le principe de l'invitation à participer à une session. C'est un protocole svelte, basé sur le texte (similaire à e-mail ou http : « *HTTP-like* »), permettant l'implémentation dans un environnement IP. A l'heure actuelle, il est moins riche que H.323 au niveau des services offerts, mais il suscite un très grand intérêt dans la communauté Internet et télécom et entre donc en concurrence directe avec H.323.

1.5.3 - Les protocoles pour terminaux simples : MCGP/MEGACO

Le protocole MGCP (« *Media Gateway to Media Controller Protocols* ») a été introduit par l'IETF. Il est complémentaire à H.323 ou SIP et traite des problèmes d'interconnexion avec le monde téléphonique.

Le protocole Megaco (« *Media Gateway Control* ») a été défini à la fois à l'IETF (RFC 3015) et à l'ITU (recommandation H.248). Il constitue une évolution de l'ancien MGCP. Comme son développé en anglais le suggère, la centralisation des fonctions téléphoniques est effectuée dans le contrôleur de passerelle de média (serveur) ; l'équipement d'utilisateur (téléphone IP et/ou passerelle de média) ne prend en charge que les fonctions de base comme le codage et la mise en paquets de la voix.

CHAPITRE 2

ANALYSE DE LA TELEPHONIE SUR IP

2.1 - La téléphonie sur IP, pourquoi maintenant ?

Depuis longtemps, les opérateurs de réseaux rêvent d'unifier les différentes technologies de réseaux afin de réduire leurs coûts. Les grandes entreprises, et encore plus les opérateurs télécom, doivent vivre avec une superposition de réseaux, fruits des investissements passés, TDM, X25, SNA, Frame Relay, ATM, IP pour ne citer qu'eux. Tout unifier sur une seule technologie, IP, promet d'énormes réductions de coût. Pourquoi donc assistons nous seulement maintenant à l'explosion de la téléphonie sur IP ? Il y deux facteurs : l'un est *technologique*, l'autre tient à la *déréglementation*.

La ToIP fait parler d'elle depuis le milieu des années 90. Elle fût d'abord présentée, par des start-up comme Net2Phone, comme moyen de téléphoner à bas coût sur Internet au moyen d'un PC. Presque 10 ans après, la technologie a considérablement mûri et les coûts ont significativement baissé. C'est ainsi qu'utiliser aujourd'hui la téléphonie sur IP est économiquement viable pour les utilisateurs.

La déréglementation est l'autre facteur majeur. Un nombre croissant de pays (États-unis, Europe, Japon) a déréglementé la boucle locale ADSL. Les opérateurs alternatifs peuvent ainsi « partager » la ligne en cuivre qui relie l'abonné et le central téléphonique. L'opérateur en titre garde le trafic téléphonique classique pendant que l'opérateur alternatif récupère tout le reste de la largeur de tuyau (bande passante) afin d'offrir un accès Internet et de la ToIP. Dès que le volume de téléphonie sur IP devient significatif, les opérateurs traditionnels réagissent et se lancent à leur tour via leur filiale de fournisseur d'accès Internet, quitte à cannibaliser ainsi leur activité de téléphonie. Dans les pays où le câble est important, les câblo-opérateurs, qui ne sont pas soumis à une forte réglementation, et ce malgré un passé peu glorieux en terme d'offres de téléphonie, s'y investissent également afin de ne pas laisser le monde ADSL les doubler.

2.2 - Les arguments qui plaident pour la Téléphonie sur IP

Pour les entreprises, le renouvellement du central téléphonique ou un déménagement peuvent être des opportunités pour adopter la voix sur IP. Mais d'autres critères sont aussi déterminants, notamment une amélioration de l'organisation du travail et une pérennité des investissements.

2.2.1 - Économiser sur la facture télécom

Le transport à moindre frais de la voix entre sites est, depuis les prémices de la technologie, le premier argument de la téléphonie sur IP. Même si ce transport n'est pas réellement gratuit et même si les coûts télécom voix ont baissé, il reste d'actualité. En effet, nombre d'entreprises ont déjà interconnecté leurs sites via des VPN/IP (« Virtual Private Network over IP ») pratiquement prêts à recevoir les nouveaux flux, tandis que les opérateurs de ces infrastructures vont parfois jusqu'à brader la bande passante. Dans le cas d'une communication via IP, les communications téléphoniques inter sites seront acheminées par le réseau informatique existant et ne sont plus facturés et il n'est facturé en terme de téléphonie que la transition sur les réseaux téléphoniques classiques. Ainsi que l'on appelle un voisin ou bien un client à l'autre bout du monde, ça ne coûtera que le prix d'une communication locale. Ces solutions s'avèrent donc beaucoup plus avantageuses si les appels téléphoniques se font sur longue distance.

Pour l'usager, l'énorme avantage de la téléphonie sur IP provient des tarifs rendus possibles par l'utilisation - totale ou partielle - de l'Internet pour acheminer les communications. Mais le potentiel est également considérable en termes de services.

2.2.2 - Pérenniser l'investissement

Un central téléphonique (PBX) est habituellement amorti sur une période de cinq à huit ans. Cependant, le basculement des entreprises vers la Téléphonie sur IP est inévitable à terme. Donc, si leurs offres traditionnelles doivent encore être conservées un certain temps au catalogue, on peut penser qu'elles disparaîtront d'ici plus ou moins cinq ans. Le remplacement d'un PBX en bout de course ou l'équipement d'un nouveau site par un central téléphonique utilisant un réseau IP local ou étendu (IPBX), représente donc un choix stratégique bien plus pérenne.

2.2.3 - Simplifier les infrastructures

Sur le réseau étendu, l'IP permet souvent une réduction du nombre de liens, notamment lorsque les anciens PBX étaient interconnectés via des liaisons louées dédiées ou des circuits virtuels Frame Relay. En effet, tous les flux passeront par un VPN/IP. Même situation sur le réseau local Ethernet sur lequel cohabiteront voix et données. À la clé, un câblage banalisé, une maintenance facilitée et une seule prise murale par utilisateur.

De plus, les Téléphones IP sont connectés directement sur le réseau informatique local existant dans les collectivités. Dans le cas d'utilisation des « hardphones », les ordinateurs sont connectés sur le téléphone IP. Ainsi aucune prise informatique supplémentaire n'est nécessaire. Il n'existe plus un réseau téléphonique et un réseau informatique mais belle et bien, un système d'information dans sa globalité

2.2.4 - Faciliter l'administration et la mobilité

Un IPBX repose souvent sur un système comme Unix, Windows, voire IOS (« Internet Operating System »), que connaissent bien les hommes de l'exploitation. Son administration s'en trouve banalisée et même centralisée : les équipements sont gérés via des interfaces standards ce qui n'est pas ou peu le cas pour un PBX. Ces interfaces sont des interfaces Web standards, qui remplacent les interfaces propriétaires des PABX. Les coûts de maintenance sont donc moins élevés et peuvent être regroupés avec les coûts de maintenance du réseau informatique.

Par ailleurs, les Téléphones IP peuvent être déplacés sans modification, le numéro de téléphone reste affecté au téléphone quelque soit la position géographique du poste IP. Le téléphone est automatiquement reconnu une fois l'utilisateur reconnecté. Ce dernier peut aussi s'identifier, même pour une durée de quelques heures, sur un autre poste. Cela permet notamment de créer rapidement des groupes de travail ou de monter ponctuellement un petit centre d'appels dans une salle de réunion. Ou encore, une entreprise peut alors conserver son numéro de téléphone, même en cas de déménagement.

2.2.5 - Homogénéiser les services téléphoniques sur un ensemble de sites

Grâce à la centralisation du gestionnaire d'appels (principal composant d'un IPBX), le moindre site distant bénéficie de la même richesse de services téléphoniques que le siège de l'entreprise. En fait, un simple lien IP suffit, dès lors que la liaison est capable de véhiculer les flux. Même le poste d'un télétravailleur sera vu et géré comme un employé normal. Cette homogénéité peut-être mise à profit pour mettre en œuvre un centre d'appels virtuel, c'est-à-dire dont les agents sont géographiquement dispersés.

2.2.6 - Faciliter l'intégration avec le système d'information

En principe, les PBX classiques permettent une intégration totale avec le système d'information, qu'il s'agisse de réaliser une messagerie unifiée, de centraliser un annuaire, ou de s'interfacer avec une application de gestion de la relation client. Mais une telle intégration a un coût, notamment lié au serveur CTI (couplage téléphonie / informatique) qui est dédié, plus ou moins propriétaire, et complexe à mettre en oeuvre.

Cette fonction est nativement présente sur la plate-forme IPBX, qui est elle-même une application parmi d'autres. Certains constructeurs commencent d'ailleurs à donner accès à ses fonctions, via le concept de services web. Les téléphones deviennent pour leur part des terminaux informatiques offrant un accès à des applications.

L'interface vocale et l'écran de taille réduite requièrent des développements certes particuliers, qui peuvent toutefois être basés sur des standards comme XML ou VoiceXML. Le terminal peut d'ailleurs être un PC multimédia. D'autre part, la mise en œuvre d'un centre de contacts gérant plusieurs médias (voix, e-mails, navigation assistée sur un site web), encore appelé web call center, devient plus naturelle. La messagerie comportera en plus des emails des messages enregistrés, la vidéo conférence se généralisera également. Ce qui, grâce aussi à l'annuaire unifié, permet d'améliorer la productivité.

En mode « *PC to PC* », les utilisateurs peuvent nativement converser à plus de deux interlocuteurs, ou associer à leur conversation d'autres modes de communication : partage d'un tableau blanc, envoi simultané d'images ou de tout autre fichier, etc. Du reste, parce qu'elles s'appuient sur des PC utilisés comme « combinés téléphoniques », de simples Web Cam connectées aux PC de chacun des correspondants permettent aux interlocuteurs de se voir, même si c'est avec une qualité d'image souvent dégradée.

Finalement, cette meilleure intégration avec le système d'information peut engendrer des gains de productivité difficiles à chiffrer, mais bien réels.

2.2.7 - Évoluer plus facilement

Dans la mesure où le gestionnaire d'appels est pratiquement en veille une fois qu'il a initialisé un appel, il peut gérer un nombre de postes très important. Tant que le réseau est en mesure d'absorber les flux, nul besoin de le mettre à niveau. Il suffit de connecter de nouveaux postes IP. Un bémol : au-delà d'un certain seuil, il faudra quand même augmenter le nombre de cartes T0 ou T2 sortant sur le réseau public. Mais on est loin des contraintes imposées par les PBX, dont l'extension par tranche et les principes tarifaires manquent de souplesse.

Par ailleurs, un réseau de type « *données* » est par nature plus évolutif qu'un réseau téléphonique classique, ce qui facilite de loin l'ajout de nouveaux services beaucoup plus riches que la téléphonie traditionnelle, d'autant plus que le téléphone IP sait interpréter la signalisation ce qui ouvre le champ à de nombreuses possibilités. Par exemple, possibilité de traitement automatique des appels :

« *<si c'est> M. Dupont <qui appelle>*
<alors répondre automatiquement>
M. Durand est actuellement absent voulez-vous laisser… »

2.2.8 - Regrouper les équipes et se passer d'un prestataire

Le passage à l'IP s'accompagne généralement d'une absorption de la téléphonie par le service informatique. Ce qui conduit à une réduction d'effectifs ou au redéploiement du personnel. Lorsque l'entreprise est trop petite pour entretenir une cellule dédiée à la téléphonie, la migration vers l'IP lui permettra de mettre fin au contrat de maintenance avec un prestataire spécialisé.

2.3 - Les faiblesses de la Téléphonie sur IP

ToIP n'a pas encore pu prendre son essor pour des raisons techniques qui constituent encore un lourd handicap. Pour gagner sa place parmi les applications d'entreprises, la technologie ToIP devra d'abord résoudre ses insuffisances techniques. Tour d'horizon de ses principaux points faibles.

2.3.1 - Fiabilité

VoIP n'est pas encore suffisamment fiable et le protocole IP en est le principal responsable. De larges segments de la population Internet utilisent des versions IP, comme la version IPv4 qui ne fournit pas un bon support pour un routage fiable. Or la question est la suivante : combien de temps accepte-t-on d'attendre la tonalité lorsque l'on décroche le téléphone ? Tant que IPv6, la future génération de protocole IP, n'est pas largement implémentée, VoIP ne sera pas une option intéressante pour les entreprises. Il faudrait l'utiliser avec d'autres solutions hybrides qui combinent l'IP avec des protocoles plus fiables, comme l'ATM. Bien qu'IPv6 soit déjà intégré à un certain nombre de solutions Internet et à des systèmes d'exploitation comme Linux, peu d'entreprises ont migré de l'IPv4 à l'IPv6. Mais cela devrait changer dans les trois années à venir, où nous assisterons à l'utilisation conjointe de IPv4 et de IPv6 sur Internet, le temps que les entreprises mettent à jour leurs équipements.

2.3.2 - *Une qualité de son médiocre*

Pour le moment, il n'y a pas de garantie de qualité sonore pour la VoIP. Elle est souvent plus mauvaise que celle d'un téléphone cellulaire utilisé dans une zone à la couverture médiocre... La qualité des liaisons téléphoniques sur réseau IP dépend en grande partie de la qualité de la maintenance et du suivi. Les temps de latence sur le réseau, la perte de paquets de données vocales, les problèmes de compression, l'écho et un résultat sonore peu fidèle affaiblissent grandement la qualité sonore de la VoIP et sont donc des paramètres à maîtriser. La tâche devrait être facilitée avec l'implémentation à grande échelle d'IPv6 d'ici les trois prochaines années, et l'intégration des dernières normes de qualité de service et des nouveaux standards par des organismes regroupant des industriels des télécoms.

2.3.3 - *Améliorer l'utilisation*

VoIP doit offrir des fonctionnalités telles que la mise en attente d'un appel et l'identification de l'appelant, des services de base de la téléphonie traditionnelle. Aujourd'hui, l'implémentation de la VoIP nécessite souvent que l'appelant tape jusqu'à 25 chiffres (numéro d'accès, numéro d'identification personnel, code et numéro de téléphone du destinataire) avant de pouvoir passer son appel. Tant que VoIP ne peut pas proposer la facilité d'utilisation et les services fournis par les systèmes vocaux traditionnels, il aura du mal à convaincre les entreprises.

2.3.4 - *Localisation*

Le nombre et la localisation des passerelles IP, qui fournissent les services de routage VoIP, limitent également le développement de la VoIP. Les fournisseurs de service doivent supporter un nombre suffisant de passerelles situées dans les zones de gros trafic pour réussir à faire des économies de coûts. Mais ce sont notamment les clients internationaux qui seront pénalisés : le manque de passerelles signifie que les fournisseurs d'accès Internet sont obligés d'acheter et de revendre des services de routage via une autre entreprise (particulièrement pour les routages longue distance). Les coûts de la solution VoIP augmentent d'autant.

2.3.5 - Standards

La ToIP dépend *principalement* du standard H.323, qui permet de mélanger la voix, la vidéo et les données. Cependant, le H.323 est un standard globalement difficile à implémenter pour les fournisseurs VoIP. Bien souvent, ils choisissent une solution propriétaire afin d'obtenir un déploiement plus rapide. Ce qui peut entraîner des problèmes d'interopérabilité pour les utilisateurs.

2.3.6 - Support administratif

Les systèmes administratifs de comptabilité, de facturation et de gestion du réseau pour la ToIP doivent être implémentés à des niveaux qui sont au moins parallèles à ceux de la téléphonie traditionnelle. Mais pour l'instant, ces derniers détiennent l'avantage dans le domaine des systèmes administratifs évolutifs qui gèrent les services administratifs.

2.3.7 - Sécurisation

Selon le *Giga Information Group*, les sociétés qui font le choix de la téléphonie IP augmentent leurs risques d'être piratées. En effet, alors que la téléphonie traditionnelle constituait un environnement isolé, la téléphonie sur IP, avec une infrastructure commune aux données, engendre bien des interrogations concernant la sécurité.

Le serveur de communication et les terminaux IP échangent trois types de flux : le premier permet le téléchargement d'une image, qui apporte le *firmware*. Le deuxième fournit les informations de configuration, qui personnalisent le poste d'un utilisateur. Le troisième concerne la communication téléphonique. Les trois peuvent comporter des brèches s'ils ne sont pas convenablement sécurisés.

Tous les fournisseurs de solutions de téléphonie sur IP s'accordent à dire qu'il faut absolument isoler les flux de téléphonie des flux concernant les données. Cela implique un environnement Ethernet commuté et non partagé, et la mise en place de réseaux locaux virtuels (ou VLAN) dont un sera dédié à la voix, avec des règles très rigoureuses pour passer d'un VLAN à l'autre. Séparer les flux vocaux des flux de données est de toute façon conseillé pour assurer une meilleure qualité de service. Pour les utilisateurs distants, la mise en place d'un réseau privé virtuel (ou VPN), généralement basé sur le protocole IPSec, s'impose.

Placés sur un PC, les téléphones IP logiciels (« softphones ») peuvent être particulièrement vulnérables. D'une part, le poste est exposé à des risques liés à des failles de son système d'exploitation, à des problèmes applicatifs ou à des virus. (Même si aucun virus visant les réseaux de téléphonie sur IP n'a été signalé jusque là, certains experts considèrent qu'il y a un risque. En effet, le fait que les téléphones IP aient leurs propres adresses IP signifie qu'ils peuvent être infectés par des virus.) D'autre part, il est exposé à toute attaque en provenance du réseau de données. C'est pourquoi, il est recommandé de protéger ses réseaux, car les attaques qui affaiblissent les réseaux, pourraient également mettre les téléphones sur IP hors service.

Cependant, des mesures de sécurité inappropriées font risquer à l'entreprise des appels longues distances non contrôlés, des conversations mises sur écoute et enregistrées à l'insu des interlocuteurs, des attaques incapacitantes (« *denial of service attacks* ») qui utilisent les ports téléphonie comme points d'entrée

La menace la plus importante est le *déni de service*. En effet, une attaque de déni de service (ou DoS, pour « *Denial of Service* ») prolongée saturera ou fera tomber le PABX-IP. C'est à la fois l'attaque qui a le plus de répercussions et celle qui est la plus facile à réaliser.

À cela s'ajoutent les craintes d'utilisation frauduleuse du système, les craintes d'écoute ou d'espionnage. Le type de fraude qui, instinctivement, fait l'objet du plus grand nombre d'investigations de la part des fraudeurs est celui qui comporte un aspect lucratif, comme téléphoner aux frais de l'entreprise.

Les intrusions pourront aussi viser à écouter les communications, enregistrer les numéros appelés, subtiliser des informations (par exemple, un vol d'annuaire), ou encore modifier des informations.

Enfin, la passerelle, qui permet de connecter le réseau IP au réseau public RTC, peut être perçue comme une porte d'entrée potentielle et des applications comme les serveurs d'appels ou la téléphonie IP offrent aussi un point d'entrée sur le réseau, semblables à des « *back doors* » et, la trace de pirates entrant par cette porte dérobée pourrait se révéler difficile à suivre.

Autre aspect à examiner, les fonctions d'administration au niveau du gestionnaire d'appels. S'il comporte un serveur Web pour la gestion à distance, il faut y accéder par l'intermédiaire d'un protocole sécurisé tel que HTTPS.

2.4 - Motivations pour la sécurisation de la ToIP

L'économie mondiale étant régie par le phénomène de la mondialisation, le monde des télécoms y cède et offre ses services. Les conséquences se reflètent au niveau technique et font ressentir le besoin urgent de trouver une solution de sécurisation de communications mondialement interopérables.

2.4.1 - Motivations techniques

Le dernier des points faibles de la ToIP, détaillé au paragraphe 2.3.7, explicite les motivations techniques à rechercher une solution de sécurisation de la ToIP. Or vu la diversification et l'émergence continues de nouveaux réseaux, ajoutées à la *déréglementation*, les recherches se trouvent de facto orientées vers le développement d'une solution indépendante de l'infrastructure (fixe ou wireless) et indépendante de la sécurisation offerte par les couches sous-jacentes. D'autant plus, que nombreuses sont les solutions qui permettent actuellement de se prémunir plus ou moins contre telle ou telle faiblesse de la ToIP ou éventuelle attaque et, il y en a même des propriétaires, mais jusque là, d'aucune n'est polyvalente, notamment en matière de sécurité.

En effet, actuellement, la sécurisation de la voix ne se fait pas de bout en bout. La figure 2.1 montre que seuls les accès des IP Phone au réseau IP ainsi que les échanges entre les terminaux mobiles et les réseaux sans fil sont sécurisés ; tous les autres échanges ayant lieu en clair.

Par ailleurs, la sécurisation actuelle de la voix n'est pas uniforme. En effet, le protocole de sécurisation de la voix, utilisé dans le cadre d'une architecture H.323 est différent de celui utilisé avec le protocole SIP et tous deux diffèrent de celui en vigueur dans le cadre des réseaux radio-mobiles.

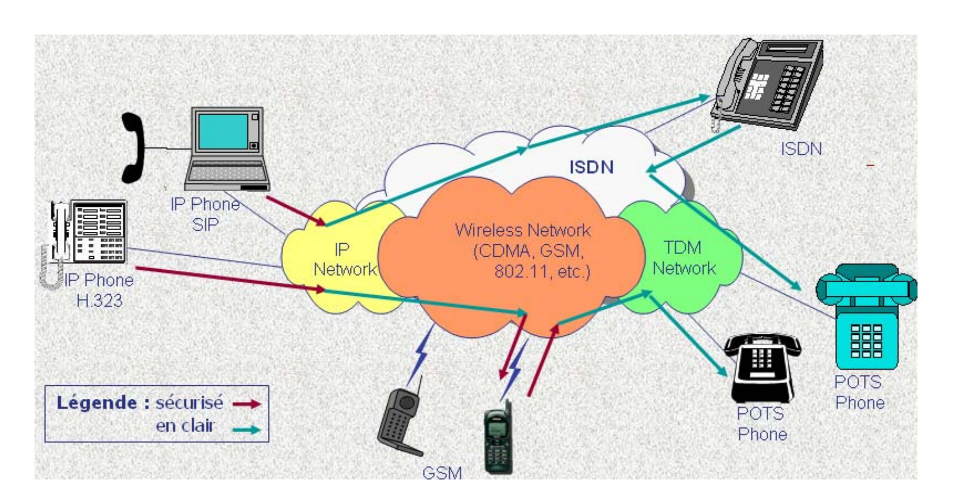


Figure 2.1 : *Schéma critique de la ToIP actuelle.*

2.4.2 - Motivations économiques

Une des principales motivations économiques pour la sécurisation de la voix indépendamment de l'infrastructure, est la guerre de l'intelligence économique qui a lieu de façon bien discrète, voire secrète et dont les conséquences sont parfois redoutables !

À ce sujet, je cite notamment l'existence du système Échelon, dont la révélation, il y a quelques années, a envenimé certaines relations au sein du monde diplomatique.

Le réseau Échelon reste l'un des secrets les mieux protégés par l'espionnage américain. Sa date de naissance précise, par exemple, est inconnue. Une certitude cependant : ce réseau mondial d'espionnage vise principalement aujourd'hui des cibles non-militaires : gouvernements, organisations, entreprises, associations ou particuliers.

Ce système, mis en place pendant la Guerre froide, permet aux agences de renseignement des États-unis et de leurs alliés – la Grande-Bretagne, le Canada, l'Australie et la Nouvelle-Zélande – de passer au crible, trier, sélectionner et analyser à l'aide d'ordinateurs puissants, chaque jour, des millions de télécopies, de télex, de messages électroniques et d'appels téléphoniques du monde entier, à la fois par origine et selon un système de mots clés figurant dans des « dictionnaires » informatiques réactualisés chaque jour par les services secrets en fonction de leurs priorités du moment, mais également d'identifier une conversation où un sujet serait abordé à mots couverts.

La figure 2.2 montre le mode de fonctionnement de ce système tant redoutable !

Tous les réseaux de communication sont donc écoutés, des câbles sous-marins (des capteurs sont déposés par des plongeurs spécialisés) au réseau Internet (la surveillance du réseau mondial est particulièrement aisée : la quasi-totalité des données transitent par des « noeuds » situés sur le territoire américain, même lorsqu'il s'agit de connexions européennes !). D'où la nécessité urgente de trouver une solution qui sécuriserait de bout-en-bout et de façon fiable des communications entre réseaux hétérogènes et qui resteraient universellement interopérables.

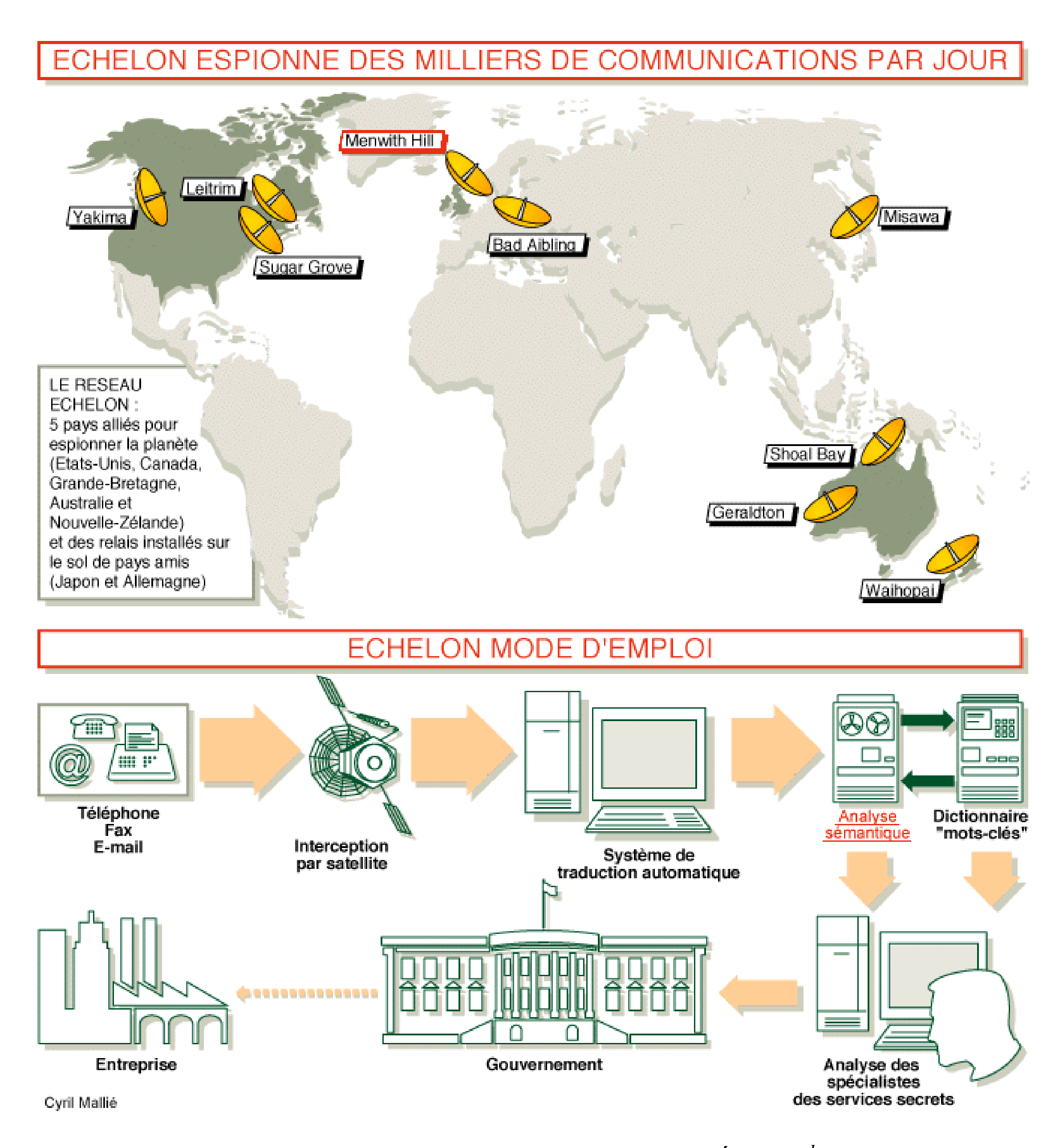


Figure 2.2 : *Fonctionnement du système Échelon*[1].

[1] MALLIÉ Cyril. Échelon : mode d'emploi. **In :** RFI. Échelon : mode d'emploi **[en ligne]**. Disponible sur : <http://cdcp.free.fr/dossiers/echelon/emploi.htm> (consulté le 22-10-2004).

2.5 - Quels services de sécurité ?

Pour permettre alors une sécurisation irréprochable de la téléphonie sur IP et surtout, indépendamment des infrastructures (fixe ou wireless) et de la sécurisation offerte par les couches sous-jacentes, la solution recherchée doit garantir cinq services de sécurité, à savoir : l'authentification, la confidentialité, l'intégrité, la non répudiation de l'appel et le non rejeu :

– l'*authentification* permet de s'assurer de l'identité de l'expéditeur du message ; qu'il est bel et bien celui qu'il prétend être ;
– la *confidentialité* permet de s'assurer qu'un message privé n'a pas pu être lu par d'autres personnes que le destinataire et ne rend donc la conversation compréhensible qu'aux seules personnes concernées. Elle est réalisée par le chiffrement de l'information échangée ;
– l'*intégrité* permet de s'assurer qu'un message n'a pas été modifié entre sa création par l'émetteur et sa lecture par le récepteur. Elle est assurée par des techniques de signature électronique (« *Digital Signature* ») ;
– le *non rejeu* ou la *protection contre le rejeu* permet de garantir qu'un adversaire ayant intercepté des messages au cours d'une communication ne pourra pas les faire passer pour des messages valides en les réinjectant sur le réseau soit dans une autre communication, soit plus tard dans la même communication. Cette garantie est assurée par l'ajout du numéro de séquence dans l'entête ;
– et enfin la *non répudiation de l'appel* permet de s'assurer qu'une transaction a effectivement eu lieu et évite donc qu'une quelconque des entités impliquées dans la communication nie avoir totalement ou en partie participé aux échanges. Cela nécessite l'archivage des données échangées.

Il est aussi à noter que la *disponibilité des ressources* pourrait également être considérée comme un mécanisme de sécurité afin de minimiser les délais et les rejets de service.

2.6 - L'avenir de la Téléphonie sur IP

Si la voix sur IP ne s'ouvre qu'aujourd'hui aux particuliers, cela fait déjà trois ans qu'elle s'est rendue indispensable à un nombre croissant d'entreprises, faisant depuis, de plus en plus d'adeptes. Cependant, malgré ses multiples services qui permettent un réel accroissement de la productivité, la demande reste prudente pour le moment. Et cela à raison.

Deux évènements ont déjà poussé les entreprises à renouveler leur parc PABX cette dernière décennie : l'introduction de la numérotation à *dix chiffres* en octobre 1996 et le *passage à l'an 2000*.

Compte tenu des durées d'amortissement et de la durée de vie moyenne des PABX en usage dans la téléphonie traditionnelle (7 ans et plus), la pénétration des PBX IP (ou IPBX) devrait être progressive et marquer une inflexion aux alentours de 2006-2007.

Au phénomène de captivité s'ajoute une certaine prudence des services généraux ou des responsables de téléphonie à se lancer dans un chantier perçu comme complexe, consommateur de ressources, n'en demeurant pas moins assez coûteux et de surcroît, présentant des risques d'attaques et des problèmes de confidentialité.

Cependant, le basculement des entreprises vers la Téléphonie sur IP est inévitable à terme, la véritable question qui se pose est de déterminer le moment propice pour entamer ce basculement, ainsi que l'approche à adopter (choix entre des solutions hybrides ou IP pur, entre un déploiement global de l'ensemble des sites, ou un déploiement progressif par plaques).

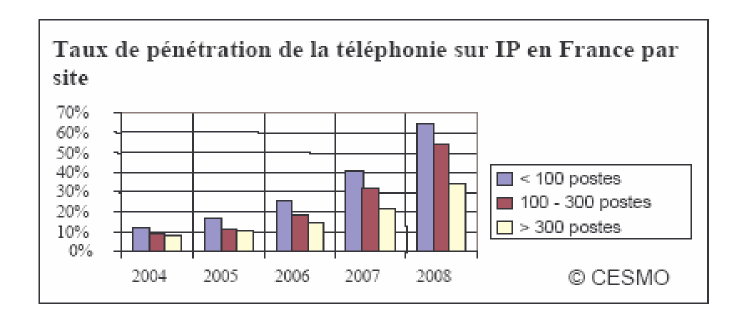


Figure 2.3 : *Perspectives de pénétration de la Téléphonie sur IP.*

D'après une étude menée par CESMO Consulting, la pénétration *moyenne* de la ToIP est estimée en 2004 à 9% et ce, sans réelle différence selon les profils de sites. Progressive jusqu'en 2006, elle devrait décoller véritablement en 2007, portée notamment par un nombre significatif prévisible de renouvellements de PABX traditionnels. Pour les sites de 300 postes, la pénétration sera supérieure à 50% en 2008.

Une autre étude menée récemment par la société britannique Analysys montre que les applications personnelles de voix sur IP menacent le cœur d'activité des opérateurs de téléphonie traditionnelle et pourraient d'ici à 2008 représenter 13%, soit 6,4 milliards d'euros, du marché résidentiel de la voix en Europe occidentale. Plus de 50 millions d'utilisateurs haut débit pourraient ainsi devenir des adeptes de la voix sur IP d'ici à 2008.

La mutation des réseaux vers le tout IP est donc une évolution normale pour les opérateurs et il est là intéressant d'être à la fois opérateur et fournisseur d'accès pour se positionner sur ce marché. Opérateur pour participer au dégroupage de la boucle locale. Fournisseur d'accès pour pouvoir développer l'offre vers le « *triple play* » (offre associant le Web, la téléphonie sur IP et la télévision). Sur ce point tout le monde est d'accord, la convergence vers le triple play, c'est l'avenir. Reste à savoir qui seront les acteurs de ce marché à la croisée de plusieurs « mondes ». Opérateurs ? Fournisseurs d'accès ? Éditeurs de logiciels ? Reste aussi à savoir comment vont réagir les opérateurs historiques, quelque peu « court-circuités » par les réseaux IP, voire l'Internet, utilisés comme réseau téléphonique.

CHAPITRE 3

L'ARCHITECTURE H.323

3.1 - La norme H.323

Le standard H.323 (« *Visual Telephone Systems and Equipment for Local Area Networks which Provide a Non-Guaranteed Quality of Service* ») porte sur la signalisation des réseaux locaux à Qualité de Service non garantie (IP est le point de mire). H.323, recommandation définie à l'origine par la Commission d'Études 16 de l'ITU-T, propose des bases pour le transport de la voix, de la vidéo et des données sur des réseaux locaux de données fonctionnant en mode sans connexion et sans garantie de qualité de service (i.e. pas de correction d'erreurs) : IP et IPX sur Ethernet, Fast Ethernet et Token Ring.

L'adoption et la promotion de H.323 comme standard pour les produits de voix/vidéo sur Internet et intranet par Microsoft et Intel, entraînant dans leur sillage des dizaines de petits éditeurs, a propulsé cette norme comme standard incontournable de la téléphonie sur Internet. Le standard s'applique désormais à tous les réseaux de paquets (ce qui inclut bien sûr Internet), et non plus seulement aux réseaux locaux.

La norme H.323 est issue de la norme H320 (visiophonie sur RNIS), et répond aux problèmes liés à IP (politique du Best Effort : pas de garantie de délais). Elle définit plusieurs protocoles et constitue donc un ensemble de recommandations venant de l'ITU-T, pour cela elle est souvent qualifiée de famille protocolaire ou même norme « parapluie ».

L'architecture H.323 fonctionne selon une stratégie bout-à-bout qui lui confère une transparence vis-à-vis des évolutions du réseau. Elle s'appuie sur des protocoles de communications (RTP, RTCP,…), mais également sur des codecs audio (G.711 obligatoire, G723.1, G.728,…) et des codecs vidéo (H.261 et H.263) et décrit aussi les terminaux, équipements, et services nécessaires à l'établissement d'une communication multimédia sur un réseau de paquets ne garantissant pas une qualité de service.

Les fonctions dédiées à H.323 sont les suivantes :

– contrôle de la procédure d'appel : requête, établissement et suivi de l'appel ;
– gestion des flux multimédias : liste de codecs recommandés ou obligatoires ;
– gestion des conférences multipoint : modèle de conférence géré par une entité centrale ;
– gestion de la bande passante : le *gatekeeper* devient un centre de contrôle et a les moyens de limiter les connexions et d'allouer la bande passante disponible ;
– interconnexion à d'autres réseaux : ATM, RNIS, RTC.

3.2 - Les différentes versions de H.323

En mai 1995 débutent les travaux sur H323. Les premiers logiciels proposant le transfert de la voix sur un réseau de transmission de données voient le jour en 1996 mais ne sont pas compatibles.

La première version de H.323 est approuvée en octobre 1996. Elle définit les standards pour les transmissions multimédias au dessus des réseaux locaux. Cependant, elle présente des points faibles tels que l'absence de la qualité de service.

La deuxième version est approuvée en janvier 1998. Elle permet une interopérabilité entre différents réseaux de paquets, offre des possibilités de connexion au réseau téléphonique traditionnel et améliore la compatibilité des équipements de téléphonie sur IP.

La troisième version de H.323 est approuvée le 30 septembre 1999. Elle introduit quelques nouvelles fonctionnalités (identification de l'appelant, communication entre *gatekeeper*, fax sur réseau de paquets, mécanisme de connexion rapide …).

La quatrième version est approuvée en novembre 2000 et apporte un meilleur niveau de fiabilité, flexibilité et passage à l'échelle. Elle s'oriente vers les URL H323, H248/MEGACO (inter fonctionnement avec MGCP), audio et vidéo sur un même canal, *gatekeeper* de secours, tunneling ISUP…

En juillet 2003 est approuvée la cinquième version de H.323. Elle décrit les composants d'un système H.323 et définit les messages de contrôle et les procédures de commande qui régissent la communication entre ces composants.

3.3 - Les éléments de H.323

Les composants d'un système H.323 sont :

– les *terminaux*, point de départ et d'arrivée d'une communication, assurent l'audio et optionnellement la vidéo et les données dans des conférences en point-à-point ou en multipoint ;
– les *gateways* assurent l'interaction avec le réseau RTC ;
– les *gatekeepers* fournissent les services de contrôle d'admission et de translation d'adresses ;
– les *Multipoint Controllers* (*MC*), les *Multipoint Processors* (*MP*) et les *Multipoint Control Units* (*MCU*) fournissent un support pour les conférences multipoints.

Les *gatekeepers*, *gateways* et *MCU* sont logiquement séparés mais peuvent être implémentés en un seul dispositif physique.

Une collection de *terminaux*, *gateways* et *MCU* gérés par un seul *gatekeeper* est appelée « *zone H.323* ». Une zone contient au moins un terminal, peut inclure des *gateways* et des *MCU* et n'a qu'un seul *gatekeeper*. H.323 se situant au niveau applicatif de l'OSI, une zone peut être distribuée sur plusieurs réseaux IP connectés par des routeurs.

3.3.1 - Les terminaux

Un terminal peut être un PC, un PDA ou tout autre périphérique autonome supportant H.323 et les communications multimédia bidirectionnelles en temps réel. Il supporte des communications audio et optionnellement des applications vidéo et/ou de données. Il peut être utilisé dans des conférences multipoints (avec un *MCU*). Son rôle est de communiquer avec d'autres terminaux multimédias (H.324 du RTC, ou H.310 (sans fil) et H.321 du B-ISDN, ou encore avec les terminaux H.320 sur RNIS ou H.322 sur un LAN avec qualité de service). Pour cela, tous les terminaux H.323 doivent supporter, en plus des codecs audio :

– *H.245*, standard de l'ITU-T, pour l'échange de capacités et la gestion des canaux logiques ;
– *RAS*, un protocole utilisé pour l'enregistrement auprès du *gatekeeper* ;
– *RTP/RTCP*, deux protocoles de l'IETF, utilisés pour le séquencement des paquets audio et vidéo. L'en-tête de RTP contient un horodatage et un numéro de séquence, permettant au dispositif récepteur de bufffériser autant que nécessaire pour supprimer la gigue et la latence lors de la synchronisation des paquets pour faire repasser un flot audio continu. RTCP contrôle RTP et recueille des informations de fiabilité qu'il repasse périodiquement aux participants à une session.

Les terminaux H.323 peuvent en plus supporter *H.225*, un standard de l'ITU-T qui utilise une variante de Q.931 pour la gestion de la signalisation des appels.

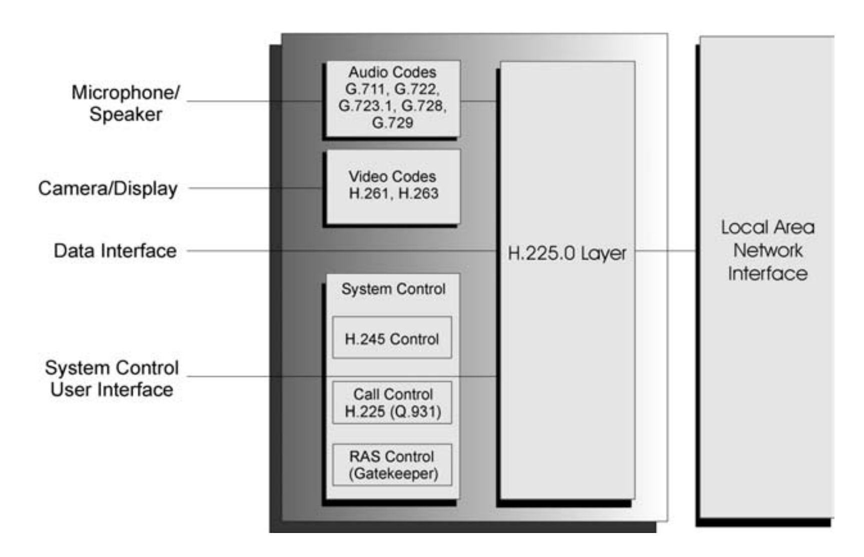


Figure 3.1 : *Décomposition fonctionnelle d'un terminal H.323.*

3.3.2 - Les « gateway »

La *gateway* est un élément optionnel puisqu'elle est utilisée pour interconnecter un réseau H.323 à un réseau non-H.323 et ne sera donc pas requise pour la communication de deux terminaux H.323. Dans le cadre de la téléphonie sur Internet, les passerelles sont utilisées pour faire le pont entre le réseau PSTN où sont connectés les postes téléphoniques (analogique classique, H.324 ; numérique, H.320) et un réseau IP. Elle comprend donc les protocoles H.323 du côté du Web et les protocoles du RTC de l'autre côté.

La *gateway* H.323 assure l'établissement et la libération des communications, durant lesquelles elle convertit un signal audio provenant du réseau IP en un signal audio analogique pour un usager du réseau téléphonique analogique ou vice-versa, et ce, en assurant la correspondance des formats de transmission (H.225.0 et H.221), celle des messages de signalisation (Q.931 et H.225), celle des procédures de contrôle (H.242/H.243 et H.245), ainsi que la cohésion entre les medias (multiplexage, correspondance des débits, transcodage audio…). Du côté du réseau public, la passerelle doit aussi supprimer les échos et du côté du réseau IP, elle doit rétablir la synchronisation du signal transféré sous forme de paquets.

La figure 4.2 explicite la fonction d'un *gateway* PSTN/IP, connectant un terminal H.323 et au réseau SCN (*Switched Circuit Network*).

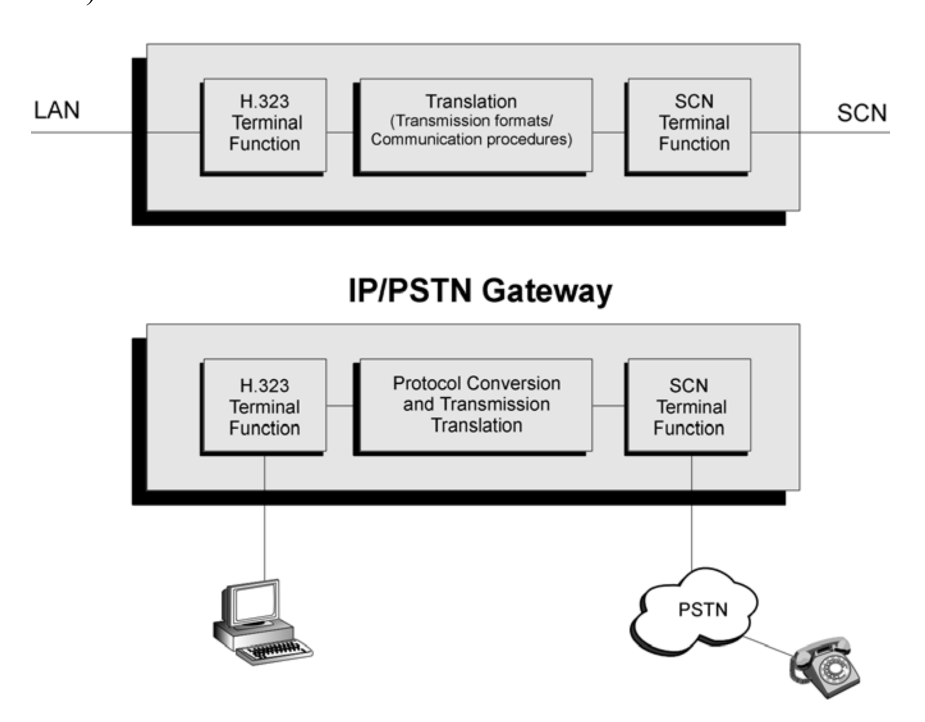


Figure 3.2 : *Décomposition fonctionnelle d'un terminal H.323.*

3.3.3 - Les « gatekeeper »

Le *gatekeeper* est un élément vital dans un système H.323. Plusieurs *gatekeepers* peuvent être présents dans une architecture H.323 pour l'équilibrage de charge (*load-balancing*), mais déjà la présence d'un seul *gatekeeper* n'est pas obligatoire. Cependant, s'il se trouve un *gatekeeper* dans une architecture H.323, il doit assurer un ensemble important de services aux éléments enregistrés auprès de lui et les terminaux doivent alors obligatoirement utiliser ces services-là.

Un *gatekeeper* agit par zone H.323 et fournit l'intelligence aux passerelles. Typiquement, il est implémenté sur PC, alors que les *gateways* sont souvent basés sur des plateformes matérielles propriétaires.

Un *gatekeeper* joue le rôle de moniteur pour tous les appels à l'intérieur de la zone H.323. Il gère les permissions pour assurer le contrôle d'admission. Quand un client H.323 veut émettre un appel, il doit le faire au travers du *gatekeeper*. C'est alors que celui-ci fournit une résolution d'adresse du client de destination par association des systèmes de numérotation intérieure et extérieure à la zone, en l'occurrence il s'agit d'une association entre un alias H.323 (l'identifiant H.323 de l'utilisateur) et une adresse IP issue du référencement du terminal, les adresses de type email ou numéro de téléphone E.164 étant possibles. Pendant la résolution d'adresse, le *gatekeeper* peut optionnellement agir en administrateur régulateur de la bande passante disponible sur le réseau.

Le *gatekeeper* assure aussi le routage des appels et la gestion des différentes *gateways* (H.320, H.324). Dans le cas où il y aurait plusieurs *gateways* sur le réseau, le *gatekeeper* peut rediriger l'appel vers un autre couple *gateway/gatekeeper* qui essaiera de le router.

Le *gatekeeper* est aussi responsable de la sécurité et de la tolérance aux pannes puisqu'il connaît à tout moment l'état et la disponibilité (ports libres) des *gateways*.

Parmi les diverses fonctions de contrôle optionnelles d'un *gatekeeper*, l'on peut citer : le rôle de proxy pour la signalisation d'appel, l'offre de services complémentaires par le biais de la signalisation d'appel, la génération d'information de gestion SNMP (services de gestion des renseignements…), la gestion des appels et l'indication d'occupation, la génération de rapports d'état et la facturation.

La signalisation entre chaque terminal et le *gatekeeper* est transmise au-dessus d'une connexion TCP, selon les spécifications de *RAS*. Un *gatekeeper* peut participer à une variété de modèles de signalisation dictés par le *gateway*. Des modèles de signalisation déterminent quels messages de signalisation passent à travers le *gatekeeper* et lesquels peuvent directement transiter entre les entités, comme le terminal et le *gateway*.

La figure 4.3 illustre un modèle de *signalisation directe* (*direct signaling*) où l'échange des messages de signalisation n'implique pas le *gatekeeper*, alors que dans un modèle de *signalisation routée* (*gatekeeper-routed signaling*) (cf. fig. 4.4) seuls les flots de média transitent directement entre les terminaux.

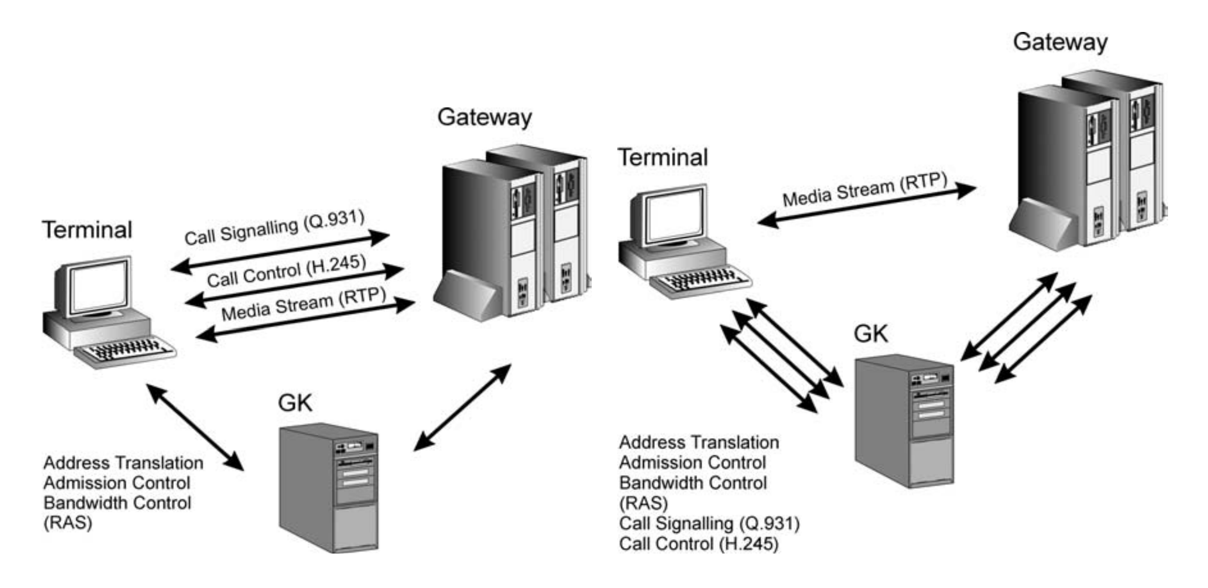


Figure 3.3 : *Signalisation directe.* ***Figure 3.4 :*** *Signalisation routée.*

3.3.4 - Les « Multipoint Control Units »

Le *MCU* (*Multipoint Control Unit*) est un élément du système H.323 permettant d'établir une conférence multipoint et avec lequel tous les terminaux participant à la conférence établissent une connexion. Un *MCU* peut constituer un dispositif indépendant ou être intégré au *gateway*, au *gatekeeper* ou au terminal et se compose logiquement d'un *MC* (*Multipoint Controller*) et d'un ou plusieurs *MP* (*Multipoint Processor*) :

– le *MC* est obligatoire. Il assure la gestion des participants (au moins trois terminaux H.323) à une conférence multipoint. Il traite les messages de signalisation et de contrôle et négocie avec tous les terminaux les moyens à mettre en œuvre pour établir des communications multimédia. Il peut également exercer un contrôle au niveau des ressources de la conférence pour déterminer par exemple l'entité qui transmet en muticast et s'il s'agit d'un flot audio ou vidéo. Il négocie en conséquence le codec à utiliser ;
– les *MP* sont optionnels. Un *MP* traite les flots de médias ou de données dans une conférence multipoint : il reçoit, mélange et synchronise les flux venant des participants, convertit les formats de données en fonction des paramètres négociés avec chaque participant et réplique les flux avant de les redistribuer aux autres participants.

Dépendamment que le *MCU* implémente ou pas de *MP*, l'on distingue trois types de conférences : *centralisée*, *décentralisée* et *hybride*. Dans une conférence *centralisée*, chaque participant ne communique qu'avec le *MCU* qui implémente les fonctions des *MC* et *MP*, alors qu'en mode *décentralisé* chaque participant communique avec le *MCU* et avec tous les autres participants, cas où le *MCU* implémente les seules fonctions du *MC* et laisse celles du *MP* à l'initiative des terminaux. En mode *hybride* on trouve des participants utilisant l'un ou l'autre mode pour se connecter à la conférence.

3.4 - La pile H.323

La pile protocolaire H.323 est indépendante des réseaux et des protocoles de transport utilisés et fonctionne selon une stratégie de bout-en-bout qui lui confère une transparence vis-à-vis des évolutions du réseau. La figure 4.5 représente la pile protocolaire H.323 dont la relation avec le modèle OSI est montrée à la figure 4.6.

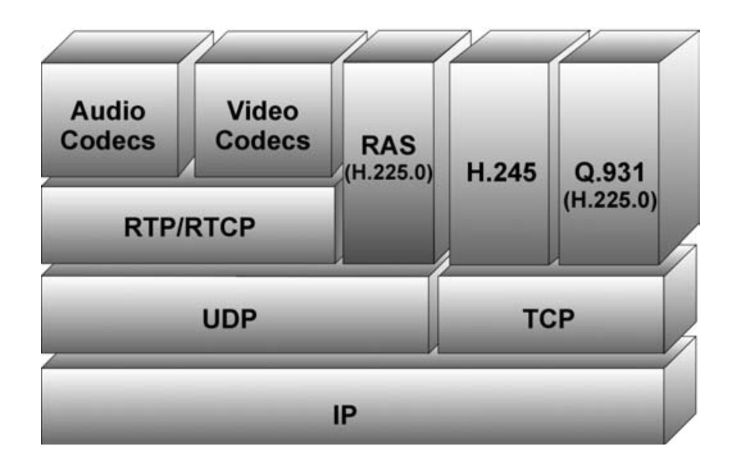


***Figure 3.5 :** Pile protocolaire H.323.*

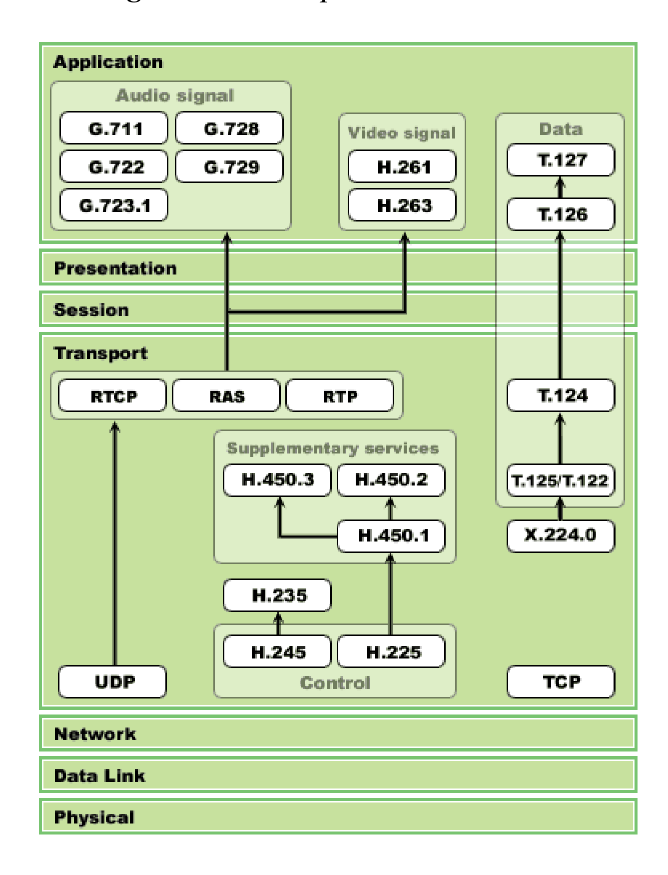


***Figure 3.6 :** Mise en évidence de la pile protocolaire H.323 par rapport au modèle OSI.*

Comme le montre la figure 3.5, si le protocole IP est utilisé (ce qui est le plus souvent le cas) alors les paquets audio, vidéo et H.225.0 RAS utilisent UDP comme protocole de transport alors que les paquets de contrôle (H.245 et H.225.0 *call signaling*), qui sont des messages importants utilisent TCP, ce qui assure leurs retransmissions si nécessaire. Les paquets de média sont transportés au-dessus de UDP car il serait inutile de les retransmettre au cas où un fragment serait perdu puisque probablement il arriverait alors assez tard pour être utilisé dans la reconstitution du message initial.

Il est à noter que des fonctions optionnelles sont également proposées dans l'architecture H.323 par les protocoles H.235 (sécurité et authentification), H.450.x (divers services supplémentaires) et H.246 pour l'interopérabilité avec les services des circuits commutés. Ci suit une description des seuls éléments obligatoires dans la constitution de la pile protocolaire H.323.

3.4.1 - Les codecs audio

Le codec audio encode le signal du microphone du terminal et décode le signal reçu pour l'envoyer vers l'écouteur. Le service audio étant le minimum commun à tous les terminaux H.323, la recommandation H.323 spécifie une série de codecs audio classés par débits allant de 5.3 à 64 kbps.

Le codec G.711 est le plus populaire conçu pour les réseaux de téléphonie. Il encode le signal selon les lois A ou U à 64 kbps et présente une très bonne qualité de restitution de la voix, bande passante élevée pour Internet. Il doit être supporté par tout terminal conforme à la norme.

D'autres codecs peuvent être optionnellement supportés, comme le G.722 (64,56 ou 48 kbps), le G.723.1 (5,3 et 6,3 kbps), le G.728 (16 kbps) et le G.729 qui utilise la quantification à prédiction linéaire pour produire une qualité supérieure à des taux de 8 et 16 kbps.

Le choix du codec dépend des exigences du réseau de transport (bande passante), de la qualité requise (service payant ou non) et de la disponibilité des codecs sur les terminaux du réseau dépendamment des constructeurs.

Actuellement, le codec G.723.1 est choisi comme celui par défaut pour les applications de téléphonie dans le monde Internet. Il est assez efficace, encode et compresse le signal vocal à 5.3 et 6.4 kbps, mais produit une restitution médiocre bien qu'intelligible.

Il est à noter qu'un terminal H.323 peut fonctionner de manière asymétrique, décodant par exemple des paquets audio G.723.1 en réception, et codant en G.711 en émission.

3.4.2 - Les codecs vidéo

De manière analogue à un codec audio, le codec vidéo encode l'image de la caméra locale et décode l'image reçue pour l'afficher sur le moniteur. La communication vidéo nécessite une bande passante importante, d'où l'intérêt d'avoir des techniques de compression et de décompression performante. Le support des codecs vidéo est alors optionnel mais tout terminal compatible H.323 et supportant la vidéo doit au minimum supporter le codec H.261 (ITU-T) qui produit la transmission vidéo pour des canaux avec une bande passante de p*64 kbps, p étant une constante qui varie de 1 à 30. H.323 spécifie aussi un autre codec, optionnel, le codec H.263, conçu pour des transmissions à faible débit sans perte de qualité.

3.4.3 - Les protocoles RTP/RTCP

Dans une visioconférence H.323, pour chaque type de média échangé (son, vidéo) et pour chaque sens de communication, un canal RTP est établi ainsi qu'un canal de contrôle RTCP (au dessus du protocole UDP). Les messages RTP sont typiquement transportés sur des ports UDP pairs, alors que les messages RTCP le sont sur les ports impairs suivants. Sous le nom global RTP on désigne à la fois les protocoles RTP et RTCP, tous deux développés dans le RFC 3550 de l'IETF ; ils ont été incorporé tels quels dans la recommandation H.323.

RTP a pour but de fournir un moyen uniforme de transmettre de bout en bout sur IP des données soumises à des contraintes de temps réel, par exemple des flux audio ou vidéo. RTP peut être véhiculé par des paquets multicast afin d'acheminer des conversations vers des destinataires multiples. Il permet d'identifier le type de l'information transportée, d'y ajouter des marqueurs temporels et des numéros de séquence et de contrôler l'arrivée à destination des paquets.

Le rôle principal de RTP consiste à mettre en oeuvre des numéros de séquence de paquets IP pour reconstituer les informations de voix ou vidéo même si le réseau sous-jacent change l'ordre des paquets, ce qui est susceptible de se produire dans la mesure où le fonctionnement d'Internet ne garantit pas que deux paquets successifs empruntent la même route. Cela permet, par exemple pour des applications vidéo, de décoder et placer au bon endroit sur l'écran chaque paquet sans attendre ses prédécesseurs et pour des applications de voix de reconstituer les échantillons de parole.

Le rôle de RTP reste donc limité : il n'a pas été conçu pour effectuer des réservations de ressources ou contrôler la qualité de service.

RTCP est un protocole de contrôle des flux RTP, permettant de véhiculer des informations basiques sur les participants d'une session et sur la qualité de service. Pour une application particulière, il peut être nécessaire de compléter RTCP par un autre protocole de contrôle.

RTCP transmet périodiquement des paquets de contrôle aux participants, utilisant les mêmes moyens de diffusion que RTP, simplement avec un numéro de port différent.

RTCP permet de recevoir des informations de retour des participants, grâce aux messages « *sender report* » et « *receiver report* ».

RTCP diffuse un identificateur pour chaque source RTP, appelé CNAME, c'est cet identificateur qui permet d'attribuer les flux RTP à tel ou tel participant, car les SSRC peuvent changer (redémarrage de programme, conflit ...). Cela permet aussi de synchroniser des flux audio et vidéo venant d'un même participant.

3.4.4 - Conférence de données

Dans le cadre d'une architecture H.323, il est possible d'échanger des données sur un canal spécifique selon la norme T.120 (au dessus du protocole de transport fiable TCP) : cette propriété optionnelle permet notamment le partage d'applications entre deux micro-ordinateurs comme un traitement de texte, un tableur ou un logiciel de présentation, ce qui s'avère très utile en pratique pour les travaux de collaboration à distance.

Il est à noter l'existence des normes T.123, T.124 et T.125 qui sont aussi utilisées dans une conférence H.323 de données.

3.4.5 - Mécanismes de contrôle et de signalisation

Le flux d'informations dans les réseaux H.323 est un mixage de paquets audio, vidéo, données et de contrôle. L'information de contrôle est essentielle pour l'établissement et la rupture des appels, l'échange et la négociation des capacités. La signalisation est indispensable pour établir une communication téléphonique. Elle permet dans un premier temps d'envoyer des messages avant la communication, d'avertir l'utilisateur et de connaître la progression de l'appel et enfin de mettre un terme à la communication. H.323 utilise trois mécanismes de contrôle et de signalisation : H.225.0 RAS, signalisation d'appel H.225 et contrôle multimédia H.245.

3.4.5.1 - H.225.0 RAS

RAS est le protocole de communication entre un *gatekeeper* et les points terminaux (terminaux et *gateways*). Il est utilisé pour l'enregistrement, l'admission et le contrôle des appels, pour gérer les variations de bande passante, l'état et le relâchement des appels entre le *gatekeeper* et les points terminaux. Un canal de signalisation RAS est ouvert entre un *gatekeeper* et un point terminal, avant l'établissement de tout autre canal afin d'acheminer les messages RAS. Le canal RAS utilise un protocole réseau non fiable (par exemple, UDP).

H225 RAS est utilisé entre un *gatekeeper* et un point terminal (terminal ou *gateway*) pour assurer les tâches suivantes :
– découverte des *gatekeeper* (*GRQ*) ;
– enregistrement des points terminaux auprès du *gatekeeper* ;
– localisation des points terminaux ;
– contrôle de l'admission ;
– jetons d'accès.

Les messages RAS peuvent être associés à des temporisateurs et des compteurs de tentatives.

3.4.5.2 - Signalisation des appels H.225

Cette signalisation est utilisée pour établir un *appel* entre deux points terminaux H.323. Bien que syntaxiquement très proche de Q.931, il s'agit ici d'un véritable établissement d'*appel* (mise en relation de deux contextes) entre application et non pas d'une *connexion* comme pour Q.931 (réservation de ressources téléphoniques dans RNIS).

H.225 est utilisé entre les points terminaux pour initialiser les appels destinés à l'acheminement de flux temps réels. Cette signalisation d'appel est échangée sur un canal de signalisation utilisant un protocole de transport réseau fiable (type TCP).

Ces messages peuvent être échangés directement entre points terminaux (*direct signaling*) ou s'il est présent, par l'intermédiaire du *gatekeeper* (*gatekeeper-routed signaling*). La méthode est déterminée par le *gatekeeper* lors d'échange de messages d'admission RAS.

3.4.5.3 - Le protocole de contrôle de signalisation H.245

La signalisation de contrôle H.245 consiste en un échange de messages de contrôle et de commandes de bout en bout entre deux points terminaux H.323 communicants ensemble. Transportés sur le canal de contrôle H.245 ouvert en permanence, contrairement aux canaux de transport des flux média, ces messages transportent les informations suivantes :
– Capacités d'échanges ;
– Ouverture et fermeture des canaux logiques de transport des flux média ;
– Gestion de contrôle de flux ;
– Commandes générales et informations.

3.5 - Séquence type d'une conversation entre deux postes H.323

Pour établir une conférence H.323 point-à-point, deux connections TCP sont requises, comme le montre la figure 3.7. D'abord, un canal Q.931 doit être ouvert avec un port bien connu de l'appelé. Les messages d'initialisation d'appel sont alors échangés comme définis dans H.225. Si l'appelé accepte l'appel, alors l'adresse IP et le port sur lesquels l'appelé doit être à l'écoute pour la connexion H.245 sont transportés à l'appelant à travers le canal Q.931.

Par la suite, l'appelant forme le canal H.245 en ouvrant une connexion TCP, utilisant pour cela l'adresse et le port indiqués. À ce moment, le canal Q.931 n'est plus exigé et peut être fermé. Le canal H.245 est alors utilisé par les deux entités pour échanger des capacités audio/vidéo et pour la détermination des maître et esclave. Finalement, quand le transfert de données est achevé, le canal H.245 peut être utilisé pour terminer l'appel.

La figure 3.7 montre un exemple de la signalisation d'appel H.323 impliquée dans un établissement d'appel réussi où les deux points terminaux de la communication sont enregistrés au même *gatekeeper* et la signalisation d'appel directe (*direct call signaling*) est utilisée.

L'établissement d'une conférence H.323 point-à-point requiert principalement cinq étapes ou phases :

– phase A : initialisation de l'appel ;
– phase B : première communication et échange de capacités ;
– phase C : établissement de la communication audiovisuelle ;
– phase D : dialogue ;
– phase E : fin.

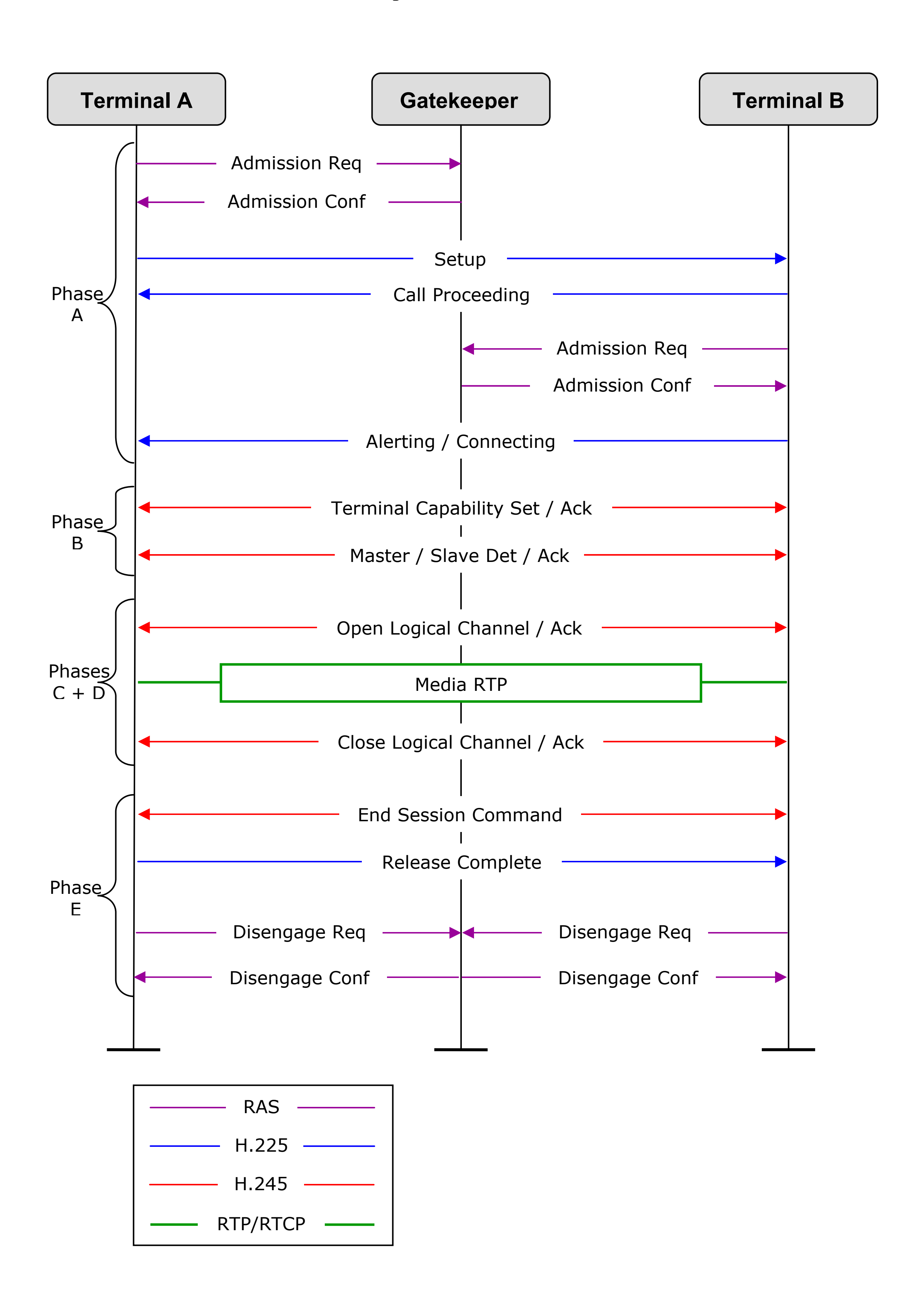


Figure 3.7 : *Signalisations d'appel H.323.*

3.5.1 - Phase A : initialisation de l'appel

L'initialisation de l'appel a lieu en utilisant les messages de contrôle d'appel H.225 (H.225 et H.225.0 RAS). Les messages RAS sont utilisés quand un *gatekeeper* est présent dans le système, autrement seulement H.225 est utilisé.

Si le *gatekeeper* n'est pas présent, alors les deux terminaux communiquent directement. Le terminal A (le terminal appelant) envoie vers le « Canal de signalisation d'appel » (*Call Signaling Channel TSAP Identifier*) (port standard TCP 1720) du poste B un message « Initialisation » (*Setup*). Ce message comprend notamment les informations suivantes :

– taux de transfert demandé au réseau, type de codage ...
– un bloc d'information User to User avec un identificateur de protocole, l'identité H.323 de la source (une chaîne de caractères), le type de la source, l'identificateur de conférence si celle-ci est en cours et si l'on veut la rejoindre, la créer ou y inviter quelqu'un, et le type d'appel (par défaut point-à-point) ;

« A » peut aussi indiquer ici une adresse de canal de contrôle (H.245) où B pourra éventuellement décider de se connecter.

B répond optionnellement par un message « Traitement d'appel en cours » (*Call Proceeding*) pour indiquer que la demande d'appel a été enregistrée qui comprend éventuellement l'adresse H.245 que A devrait utiliser pour se connecter sur B, et émet encore optionnellement un message « Sonnerie » (*Alerting*) pour indiquer que l'utilisateur B est en train d'être alerté.

Enfin B termine par un message « Connexion » (*Connect*) qui comprend notamment :

– la référence de l'appel (identificateur unique de cet appel) ;
– les capacités de transfert requises selon la norme RNIS I.231 (taux de
– transfert demandé au réseau, type de codage...), informations obligatoires seulement lors d'un appel vers un *gateway* donnant accès au RTC ou au RNIS ;
– indicateur de progrès ;
– date/heure ;
– un bloc d'information User avec l'adresse de transport H.245 que A doit employer pour négocier les capacités, le Type de Destinataire, l'éventuel numéro d'identificateur de conférence.

Quand un *gatekeeper* est utilisé, il peut y avoir plusieurs configurations possibles puisque les terminaux peuvent être enregistrés au même *gatekeeper* ou à des *gatekeepers* différents, de même qu'il se peut qu'un seul terminal seulement soit enregistré à un *gatekeeper*. Il est également possible que le *gatekeeper* fonctionne soit en mode de signalisation directe (*Direct Call Signaling*) ou routée (*Routed Call Signaling*). La figure 3.7 montre un exemple d'établissement réussi d'appel où les deux terminaux sont enregistrés au même *gatekeeper* et où la signalisation d'appel utilisée est directe.

« A » initie l'échange d'*ARQ/ACF* (*Admission ReQuest / Admission ConFirm*) avec ce *gatekeeper*, qui renvoie l'adresse de transport du canal de signalisation d'appel (*Call Signaling Channel Transport Address*) de B dans l'*ACF*.

« A » utilise alors cette adresse pour envoyer le message *Setup* à B qui si tout va bien accepte l'appel et initie un échange d'*ARQ/ACF* avec le *gatekeeper*. B répond avec le message *Connect* qui contient une adresse de transport du canal de contrôle (*Control Channel Transport Address*) de H.245 que A devra utiliser dans la signalisation H.245.

Quand l'appel devrait être initialisé par l'intermédiaire d'un *gateway* ou d'un *MCU*, l'initialisation d'appel entre le *gateway* ou le *MCU* et le terminal suit une structure tout à fait semblable au scénario d'initialisation d'appel entre deux terminaux, présentée ci-dessus.

3.5.2 - Phase B : première communication et échange de capacités

Une fois que les deux terminaux ont échangé les messages d'initialisation d'appel, ils doivent établir le canal de contrôle de H.245, qui sera utilisé pour l'échange de capacités (*Capabilities*) et l'établissement du canal des médias.

« A » ouvre alors un canal de contrôle H.245 vers B (ou B vers A en utilisant l'adresse du message *Setup*). Ce canal est unique pour chaque appel d'un terminal à l'autre, même si cet appel met en jeux plusieurs flux audio (langues) et/ou vidéo. Le numéro logique H.245 de ce canal est toujours 0.

Soit ce canal H.245 est ouvert par B lorsqu'il reçoit le message *Setup*, soit il est ouvert par A lors de la réception du message *Alerting* ou *Call Proceeding*. L'adresse et le port à employer ont été donnés dans l'un de ces messages.

Le premier message H.245 envoyé est *Terminal Capability Set*, qui comprend notamment les informations suivantes :

– un numéro de séquence ;
– les capacités de multiplexage de flux (*Stream Multiplex Capabilities*) ;
– table de capacités (*Capabilities Table*) : contient les possibilités d'échange et de compression audio ou vidéo, de chiffrement et d'échange de données : par exemple type de codages vidéo acceptés, types de codage audio, paramètres de la norme d'échange de données T.120.

Chaque terminal envoie ce message à l'autre. À la réception du message, A et B accusent réception par un message *Terminal Capability Ack*. Ils déterminent ensuite qui sera le maître dans la conversation grâce à un échange de messages H.245 *Master / Slave Det / Ack*. Cela sert à résoudre les conflits au cas où les deux terminaux chercheraient simultanément à devenir MC (*Multipoint Controler*) ou à ouvrir l'un vers l'autre et simultanément un canal bidirectionnel.

3.5.3 - Phase C : établissement de la communication audiovisuelle

Les paquets de données voix et image vont circuler dans plusieurs « canaux logiques » H.245. Sauf pour les éventuelles données T.120, ces canaux sont unidirectionnels.

« A » ouvre donc un canal logique vers B pour le son. Il envoie pour cela un message H.245 *Open Logical Channel* qui contient le numéro qui sera attribué au canal H.245 à ouvrir et les paramètres correspondant (numéro de port, type de données (par exemple, audio G.711), et les paramètres additionnels que sont, par exemple pour des données H.225.0, le numéro de session RTP, l'adresse de transport pour les données de retour RTCP (adresse IP + port) unicast ou multicast, le type de données RTP, et si l'émetteur cesse d'émettre pendant les silences).

B renvoie *Open Logical Channel Ack* pour ce numéro de canal H.245, il y mentionne le port UDP où A peut envoyer ses données RTP, et le port TCP où A peut envoyer ses données de contrôle RTCP.

B ouvre à son tour un canal et A confirme.

3.5.4 - Phase D : dialogue

A et B « parlent », les paquets sont échangés sur les canaux virtuels établis précédemment selon le protocole RTP/RTCP repris par H.225.0. Plus précisément, les données RTP circulent vers le numéro de port précisé dans *Open Logical Channel*, et les données RTCP sur le port suivant.

Il est à noter qu'il y a plusieurs services d'appel applicables qui sont inclus dans les spécifications H.323 comme les variations de la bande passante, le statut et la conférence ad hoc.

La bande passante de l'appel est initialement négociée et fournie par le *gatekeeper* pendant la phase d'initialisation de l'appel, mais à tout moment pendant un appel, le terminal ou le *gatekeeper* peut en demander une augmentation ou une diminution.

Si le changement résultera en un débit binaire global excédant la largeur de bande de l'appel courant, le terminal demanderait un changement de la largeur de bande d'appel de son *gatekeeper*. Un changement de largeur de bande pourrait être utile si un terminal utilise une bande passante réduite pendant une période de temps prolongée, libérant ainsi de la bande passante pour d'autres appels.

Dans l'exemple de la figure 3.7, A demanderait un changement de bande passante avec *BRQ* (*Bandwidth Change Request*) au *gatekeeper* qui répondrait par l'envoi de *BCF* (*Bandwidth Change Confirm*). Quand la bande passante de l'appel est suffisante pour supporter le changement, A ferme et rouvre le canal logique, spécifiant le nouveau débit binaire en envoyant des messages *closeLogicalChannel* et *openLogicalChannel* à B qui demande alors un changement de la bande passante de l'appel avec son *gatekeeper* avant d'envoyer à A un *openLogicalChannelAck*.

3.5.5 - Phase E : fin

Dans l'exemple de la figure 3.7, quand l'un des terminaux souhaite terminer l'appel, il commence par fermer d'abord tous ses canaux logiques pour la vidéo, les données et l'audio, grâce au message H.245 *closeLogicalChannel* correspondant au numéro de canal ouvert et qui sera acquitté par un message *closeLogicalChannelAck*. Par la suite, il envoie un message H.245 *endSessionCommand*, attend de recevoir le même message de son interlocuteur et ferme le canal de contrôle H.245.

Si un canal de signalisation d'appel H.225 a été ouvert, chaque terminal doit envoyer un message *ReleaseComplete* avant de le fermer.

Du moment où un *gatekeeper* est présent, il doit être mis au courant de la libération de la bande passante. Pour cela, les terminaux doivent se désengager de leur *gatekeeper* en utilisant le message *Disengage Request*. Le *gatekeeper* répond alors par un *Disengage Confirm* et l'appel est terminé.

CHAPITRE 4

ARCHITECTURES ET SOLUTIONS PERSPECTIVES

4.1 - Architectures de ToIP

En offrant la possibilité de faire transiter les communications voix sur des réseaux de données, la ToIP marque la fin d'une cohabitation entre deux réseaux distincts, très différents, du point de vue de la gestion et de la technologie. Ce transfert de l'ensemble des flux sur une infrastructure unique marque les prémices d'une convergence des réseaux multiservices existants (voix, données, vidéo).

Trois grandes familles de ToIP traduisent le taux de convergence des réseaux voix-données :

- la famille « de poste informatique à poste informatique » ;
- la famille « de poste informatique à téléphone » ;
- la famille « de téléphone à téléphone ».

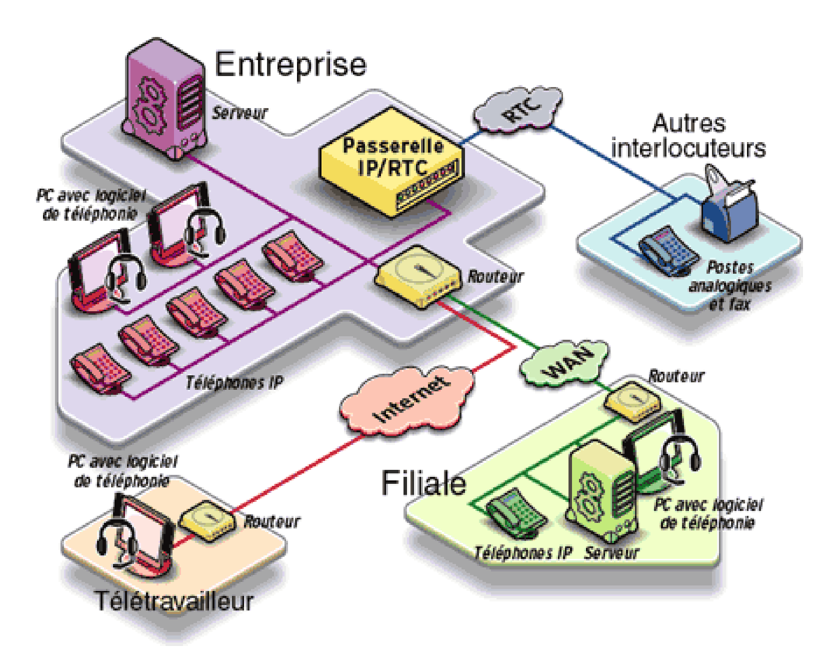


Figure 4.1 : *Convergence des réseaux voix-données.*

4.1.1 - De poste informatique à poste informatique

Cela nécessite que les deux interlocuteurs soient équipés informatiquement et dialoguent en utilisant absolument le même logiciel et pour cela évidemment un simple micro et des hauts parleurs. Ce genre de communication est gratuite exception faite du coût du logiciel.

L'intérêt de ce type de communication se trouve dans la Visio Conférence, les ordinateurs se connaissent par leurs adresses IP. Or, les adresses IP changeant à chaque connexion, les correspondants doivent se mettre d'accord sur la consultation d'un annuaire (« dynamique », car mis à jour à chaque connexion par chaque correspondant potentiel qui doit s'y enregistrer) pour permettre à l'appelant de connaître l'adresse de l'appelé (cette procédure est grandement facilitée pour des utilisateurs connectés en permanence à Internet).

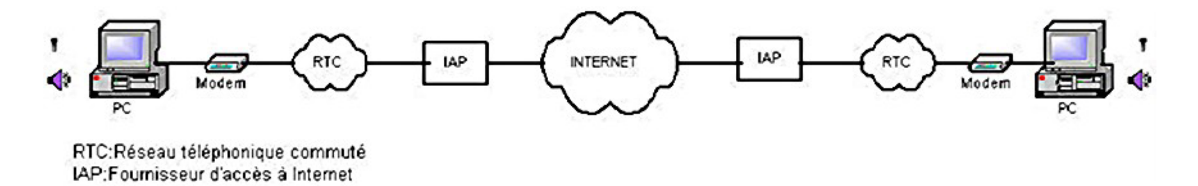


Figure 4.2 : *Téléphonie entre postes informatiques.*

4.1.2 - De Poste informatique à téléphone (ou vice-versa)

L'un des correspondants est sur son micro-ordinateur ; s'il désire appeler un correspondant sur le poste téléphonique de celui-ci, il doit se connecter sur un service spécial sur Internet, offert par un fournisseur de service (un ISP) ou par son fournisseur d'accès à Internet (son IAP), mais qui doit mettre en œuvre une *gateway* (passerelle) avec le réseau téléphonique. Cela nécessite la mise en oeuvre d'une passerelle soit au départ de l'appel soit a l'arrivée pour assurer la traduction entre les éléments spécifiques des deux réseaux (signalisation, codecs, formats de transmission d'information) afin de faire transiter la communication d'un réseau IP à un réseau téléphonique.

Si le correspondant qui appelle est sur son poste téléphonique et qu'il veut joindre un correspondant sur Internet, il devra appeler le numéro spécial d'une passerelle qui gérera l'établissement de la communication avec le réseau Internet et le correspondant sur ce réseau pourvu, là aussi, qu'il soit au rendez-vous (à moins qu'il ne soit connecté en permanence).

L'appel est taxé uniquement pour la traversée du réseau téléphonique. Ainsi, pour les appels internationaux, plus la proportion du segment IP est grande, plus l'économie réalisée sera importante.

L'intérêt de cette famille de communication réside dans le *tout-IP* (ou « *full-IP* ») : la configuration ne se borne pas à l'interconnexion de PBX (« *Private Branch eXchange* »), tous les éléments peuvent se contacter. Le réseau IP doit pouvoir supporter un certain niveau de qualité de service.

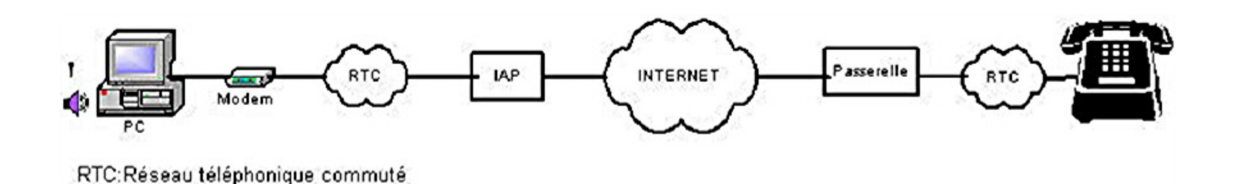


Figure 4.3 : *Téléphonie entre poste informatique et téléphone.*

Les solutions tout-IP se regroupent en deux types d'architectures :

- l'architecture de ToIP *locale*, qui peut s'utiliser pour une nouvelle infrastructure (nouvel immeuble par exemple avec uniquement du câblage catégorie 5 ou 6) ;
- l'architecture de ToIP *distante*, elle, s'utilise en multi-sites tout-IP avec l'aide d'un opérateur adéquat et parfois des serveurs centralisés. L'idée déjà ancienne d'externaliser la fonction remplie par le PBX est placée sous le terme générique de *centrex*. Les centrex IP facilitent la mise en œuvre de fonctions mixant informatique et téléphonie, la première de ces applications mixtes est la messagerie unifiée – les messages vocaux étant traduits en fichiers sonores et envoyés sur des adresses e-mails.

4.1.3 - De téléphone à téléphone

Lorsque l'appelant et l'appelé sont tous les deux sur téléphone, le réseau de transport devient transparent, cela nécessite la mise en oeuvre de plusieurs passerelles qui s'occupent alors de la gestion de la communication, y compris la signalisation avec le réseau téléphonique et les conversions à l'entrée et à la sortie du réseau IP.

Cette architecture est dite *hybride* (circuit / Voix sur IP). Elle est intéressante pour l'interconnexion de PABX : remplacement d'une ligne louée de type RNIS par une architecture réseau assurant une qualité de service, tout en préservant l'architecture téléphonique globale. La tarification dépend de l'opérateur ; s'il s'agit d'un réseau privé, c'est gratuit. Les téléphones classiques (non « IP-phone ») ne peuvent contacter les ordinateurs.

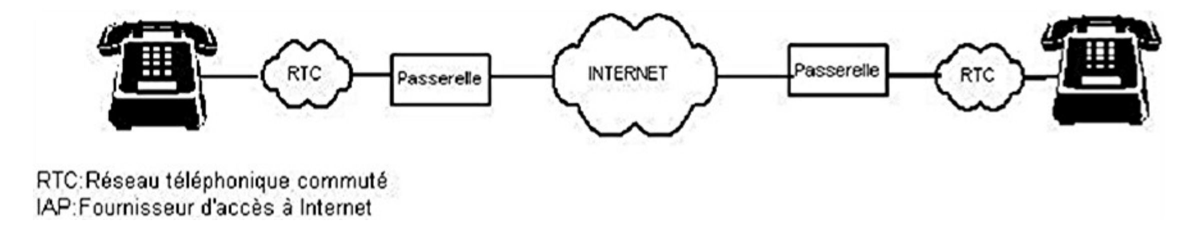


Figure 4.4 : *Téléphonie entre postes de téléphones.*

4.2 - Analyse du modèle d'appel et de l'architecture

Pour pouvoir proposer une architecture de sécurité aux communications de voix, nous allons commencer par définir les différents modèles d'appels utilisés en téléphonie. En principe, pour acheminer des données entre deux usagers, une communication est établie entre les deux entités comme suit :

– un (des) canal(aux) (physique ou logique) est(sont) établi(s) entre deux usagers qui sera(seront) utilisé(s) pour acheminer les échantillons de voix pour toute la durée de la communication. Nous pouvons donner en exemple deux usagers connectés entre eux par le réseau téléphonique commuté/réseau GSM, ou connectés entre eux à travers le réseau Internet pour un appel de voix sur IP ;
– une communication est établie entre les deux usagers distants en passant au préalable à travers un ou plusieurs équipements intermédiaires auquel(auxquels) au moins un des deux communicants est connecté. Cet équipement intermédiaire peut être un PABX conventionnel interne d'une entreprise ou bien une passerelle de voix sur IP.

Afin de sécuriser l'appel de voix entre deux communicants, il faut s'assurer du modèle d'appel utilisé et des vulnérabilités relatives aux infrastructures mises en œuvre pour effectuer ce modèle de communication.

Comme un appel peut passer au travers d'infrastructures hétérogènes, il est alors nécessaire de faire abstraction de l'infrastructure sous-jacente et d'assurer une sécurisation de la communication indépendamment des techniques déployées pour établir l'appel.

Les aspects de sécurité entrent en jeu lorsqu'il est nécessaire ou préférable de protéger l'information transmise d'un adversaire qui pourrait menacer la confidentialité, l'authenticité, l'intégrité, etc. Toutes les techniques de sécurité ont deux composantes :

– une transformation relative à la sécurité de l'information à envoyer par chiffrement des messages ;
– une information secrète partagée par les deux acteurs, et de préférence, inconnue d'un éventuel adversaire. Une clé de chiffrement utilisée pour le brouillage des messages à l'émission et leur décodage à la réception.

Une tierce partie de confiance peut s'avérer nécessaire pour réaliser une transmission sûre. Elle peut, par exemple, être responsable de la distribution de l'information secrète aux deux acteurs tout en la préservant de toute agression. Elle peut jouer le rôle de l'arbitre entre deux acteurs en dispute concernant l'authenticité et la non-répudiation de la communication.

Des politiques de sécurité qui gère les mécanismes de sécurité à appliquer à un appel suivant les nécessités et les requis du type de l'appel doivent être aussi définies.

4.3 - Solutions perspectives pour la sécurisation de la VoIP

La figure 4.5 montre les différents protocoles de sécurité utilisés pour transporter et sécuriser une communication VoIP basée sur les normes de la famille H.323. H.235 définit les conditions de sécurité dans un environnement H.323 où TLS est utilisé pour sécuriser le canal de signalisation. Le trafic de voix se sert du transport RTP pour des communications de bout-en-bout entre des points terminaux. Par conséquent, il peut utiliser SRTP pour sécuriser les paquets de voix. Les trafics de signalisation et de voix peuvent être sécurisés avec IPSec.

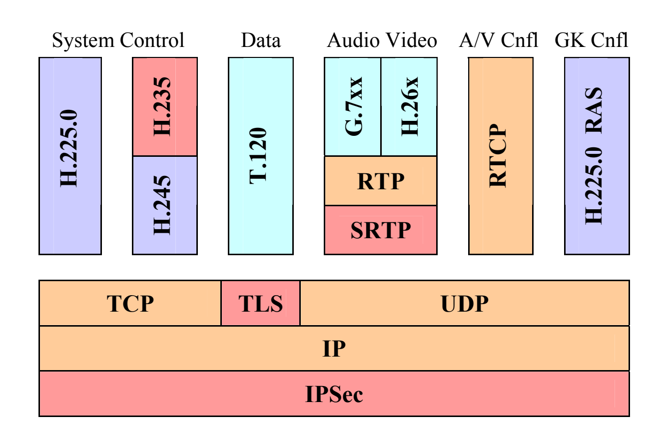


Figure 4.5 : *La pile H.323 avec les différents protocoles de sécurité.*

4.3.1 - La sécurité avec H.235

H.235 est la partie sécurité du standard H.323, préparé par le groupe d'études numéro 16 de l'ITU-T. Son but est de fournir un support pour les fonctionnalités essentielles de sécurité dans les communications H.323, comme l'*authentification*, la *confidentialité*, l'*intégrité* et parfois la *non répudiation*, dépendamment du profil utilisé.

En effet, la recommandation H.235 propose en annexe des profils de sécurité qui utilisent les champs de H.235 pour fournir des services de sécurité au trafic H.323 en se basant sur des clés symétriques, sur des signatures digitales, ou sur des PKI.

Les mécanismes de sécurité offerts par H.325 sont détaillés au paragraphe 6.2 dans le cadre d'une étude comparative entre les mécanismes de sécurité offerts par FNBDT et ceux offerts par SRTP, où H.235 est pris comme élément référence de la comparaison.

Il est à noter qu'en plus de la protection du trafic de voix lui-même, H.235 assure la protection de la signalisation d'appel H.225, du contrôle d'appel H.245 et de la signalisation RAS.

Cependant, cette recommandation n'est pas un standard de sécurité en elle-même. Pour assurer des mécanismes de sécurité pour la voix et pour la signalisation, elle repose sur des solutions de sécurité déjà existantes, comme IPSec ou TLS et de plus, elle ne traite pas tous les problèmes de la sécurité.

4.3.2 - La sécurité avec IPSec

Le protocole IPSec est une suite de protocoles désignés pour sécuriser les communications au niveau de la couche réseau. La suite de protocoles est constamment en évolution depuis 1995. De nouveaux drafts sont proposés au sein du groupe de travail à l'IETF. IPSec propose deux protocoles de sécurité du trafic IP : *Authentication Header* (*AH*) et *Encapsulating Security Payload* (*ESP*).

Chaque protocole AH ou ESP peut fonctionner en mode transport ou en mode tunnel :

- le mode *transport* réalise une simple encapsulation sans changement d'entête. Ce mode protège uniquement le contenu du paquet IP et pas son en-tête. Il n'est utilisable que sur les équipements terminaux (serveurs, postes clients) ;
- le mode *tunnel* est utilisé par les équipements réseaux pour les applications VPN. Il réalise une encapsulation plus complète avec changement de l'entête d'origine du datagramme. Ce mode protège la totalité du paquet IP.

Ci suit les services de sécurité offerts par les deux protocoles de IPSec :

- en ce qui concerne l'*authentification* des données, elle est assurée de la même façon avec AH et ESP à la seule différence que dans le mode *transport* de ESP, l'entête IP est transmise en clair et n'est pas couverte par la fonction d'authentification. Voici alors comment est assurée l'*authentification* des données avec le protocole AH : elle l'est par le mécanisme de l'entête AH (champ donnée d'authentification, etc.). AH calcule une fonction d'authentification sur tout le datagramme IP en utilisant une clé secrète d'authentification. L'algorithme d'authentification appliqué est négocié dans une association de sécurité. L'émetteur calcule une donnée d'authentification avant d'envoyer le paquet IP authentifié. Le récepteur vérifie les données authentifiées à la réception. Certains champs du paquet IP (TTL (IPv4), Hop Limit (IPv6)) en transit sur le parcours entre l'émetteur et le récepteur et qui doivent changer de valeur ne seront pas inclus dans le calcul de la fonction d'authentification assurée par le protocole AH. Ces champs-là n'influencent pas la sécurité assurée au paquet authentifié. L'algorithme d'authentification par défaut utilisé par AH est le MD5. L'utilisation de AH augmente le temps de traitement au niveau du processeur ainsi que le délai dû au calcul des données d'authentification par l'émetteur et au calcul et comparaison des données d'authentification par le récepteur ;

- seulement le protocole ESP assure la *confidentialité* et ce par le chiffrement des données utiles jusqu'au champ *NEXT* inclus (ce champ contient un identifiant du protocole de niveau supérieur). L'algorithme de cryptage appliqué est négocié dans une association de sécurité. ESP est désigné pour être utilisé avec des algorithmes de cryptage symétrique. Puisque les paquets IP n'arrivent pas en séquence chez le récepteur, chaque paquet IP doit transporter des données spécifiques de synchronisation cryptographique nécessaires au déchiffrement. L'algorithme de cryptage utilisé peut être par bloc ou par flux. ESP introduit de la complexité au niveau de l'utilisateur lors de son implémentation ;
- les deux protocoles AH et ESP assure l'intégrité de la même façon, en mode non connecté. Elle est obtenue par calcul de la valeur d'un ICV (*Integrity Check Value*) sur certains champs de l'entête IP, sur l'entête AH (ou ESP) et sur les protocoles de niveau supérieur encapsulés dans ce paquet IPSec. L'algorithme utilisé pour le calcul de ICV est basé sur un algorithme à clé symétrique (DES) ou sur une fonction de hachage à sens unidirectionnel (MD5 ou SHA-1) ;
- la *protection contre le rejeu* est définie dans IPSec de façon optionnelle : elle est négociée à la demande du récepteur dans une association de sécurité et est assurée de la même façon avec AH et ESP par le numéro de séquence inclus dans l'entête de AH (ou ESP). Ce numéro s'incrémente avec chaque émission d'un paquet IPSec ;
- seulement le protocole AH garantit la *non-répudiation*, qui peut être présente par l'utilisation de certains algorithmes d'authentification (algorithme aysmétrique RSA où les clés de l'émetteur et du récepteur sont utilisées dans le calcul des données d'authentification) lors de l'application du protocole.

Il est à signaler qu'une implémentation IPsec gère une base de données des associations de sécurité (SAs). Une association de sécurité détient la façon de traiter un paquet IP, elle est unidirectionnelle. Pour assurer la sécurité de la communication entre deux entités, deux associations de sécurité seront négociées. Les informations incluent des paramètres tels la transformée de cryptage et les clés, etc.

Par ailleurs, deux facteurs principaux affectent la transmission de la voix quand IPSec est utilisé :

- l'augmentation de la taille des paquets, essentiellement causée par les en-têtes ESP et le nouvel en-tête IP nécessaire pour le tunnel ;
- le temps nécessaire pour crypter les en-têtes et les données utiles et la construction de nouveaux paquets.

D'un point de vue pratique, IPSec est un protocole relativement difficile à implémenter d'une part à cause de sa complexité intrinsèque (multiples sous-protocoles...) et d'autre part à cause de ses interactions avec les processus réseaux courants. Cela rend ce standard assez lourd et compliqué à implémenter et à maintenir dans un environnement de la téléphonie sur IP.

4.3.3 - La sécurité avec TLS

Le protocole de sécurité de la couche transport (TLS) est une norme ouverte de l'IETF, conséquence naturelle de SSL (*Secure Sockets Layer*). TLS repose actuellement au-dessus de la couche transport et fournit la sécurité du niveau applicatif pour les communications. Un avantage de TLS est qu'il est indépendant du protocole d'application. TLS fournit des facilités pour l'authentification, l'intégrité et l'intimité entre les entités communicantes.

L'utilisation de TLS exige un mécanisme fiable de transport tel que le TCP et donc TLS ne fonctionne pas au-dessus de UDP. L'implication évidente pour la téléphonie sur IP est la signalisation basée sur TCP et d'autres communications hors-bande peuvent se servir de TLS mais la signalisation non basée sur TCP et les flots de médias basés sur UDP ne le peuvent pas. Puisqu'il exige une couche de transport sous-jacente appropriée (c.-à-d. pas UDP), TLS ne peut pas sécuriser le flot de médias.

Les protocoles de niveau plus élevé peuvent reposer sur le protocole TLS d'une manière transparente. La norme TLS, cependant, n'indique pas comment les protocoles ajoutent la sécurité avec TLS ; les décisions sur la façon d'initier le *handshaking* de TLS et la façon d'interpréter les certificats d'authentification échangés sont laissées au jugement des concepteurs et de ceux qui implémentent des protocoles fonctionnant au-dessus de TLS.

TLS soutient trois modes d'*authentification* :
– l'authentification des deux parties ;
– l'authentification du serveur avec un client non authentifié ;
– et l'anonymat total.

Si le serveur est authentifié, son message de certificat doit fournir une chaîne de certificat valide, menant à une autorité de certification acceptable. De même, les clients authentifiés doivent fournir au serveur un certificat acceptable. Chaque partie est responsable de vérifier que le certificat de l'autre est valide et n'a pas expiré ou été révoqué.

Le but premier du protocole TLS est de fournir l'intimité et l'intégrité des données entre deux applications communicantes. Le protocole se compose de deux couches : le protocole *TLS Record* et le protocole *TLS Handshake*. Au niveau le plus bas, reposant sur un certain protocole de transport fiable (par exemple, TCP), se trouve le protocole *TLS Record*. Il fournit la sécurité de connexion qui a deux propriétés de base :

– *confidentialité* : la cryptographie symétrique est utilisée pour le chiffrement des données (par exemple, DES, etc.) Les clefs pour ce chiffrement symétrique sont produites de façon unique pour chaque connexion et sont basées sur un secret négocié par un autre protocole (tel que le protocole *TLS Handshake*). Le protocole *TLS Record* peut également être utilisé sans chiffrement ;

– *intégrité* : le transport de messages inclut un contrôle d'intégrité de message en utilisant une fonction MAC (*Message Authentication Code*) à clé. Les fonctions sécurisées de hachage (par exemple, SHA, MD5, etc.) sont utilisées pour des calculs de MAC. Le protocole *TLS Record* peut fonctionner sans MAC, mais est généralement utilisé seulement en ce mode, alors qu'un autre protocole utilise le protocole *Record* comme un transport pour les paramètres de négociation de sécurité.

Les données sortantes sont protégées avec un MAC avant transmission. Pour protéger le message des attaques par rejeu ou par modification, le MAC est calculé à partir du secret du MAC, du numéro de séquence, de la longueur du message, du contenu du message et de deux chaînes fixes de caractères. Le champ du type du message est nécessaire pour garantir que les messages prévus pour un client de la couche *TLS Record* ne soient pas réorientés vers un autre client. Le numéro de séquence garantit que les tentatives de suppression ou réordonnancement des messages seront détectées.

La *non répudiation* n'est pas spécifiée dans TLS, elle pourrait cependant être fournie par l'utilisation d'un certain algorithme tel que RSA.

4.3.4 - La sécurité avec SRTP

SRTP (*Secure Real-time Transport Protocol*) est un profil et une amélioration du standard RTP pour assurer la confidentialité, l'intégrité et l'authentification des messages et la protection contre le rejeu. SRTP est un nouveau mécanisme de sécurité considéré pour sécuriser les réseaux de Voix sur IP. SRTP crypte les données utiles d'un paquet VoIP (payload d'un paquet RTP) mais garde l'en-tête en clair. Il ne crypte pas les paquets de signalisation de la voix. Le but de SRTP est d'assurer la confidentialité des champs utiles des paquets RTP et RTCP, l'intégrité de tout le paquet RTP et RTCP avec protection contre le rejeu. Ces services de sécurité sont optionnels et mutuellement indépendants. Seule la protection de l'intégrité des paquets RTCP est obligatoire pour éviter la perturbation du flux RTP. SRTP est indépendant des couches sous-jacentes utilisées par RTP. SRTP est caractérisé par un débit élevé et une faible expansion des paquets. SRTP utilise le *additive stream cypher* comme outil de cryptage, une fonction de hachage universelle pour l'authentification des messages et un numéro de séquence implicite pour le séquencement basé sur le numéro de séquence des en-têtes du paquet RTP.

Les mécanismes de sécurité offerts par SRTP sont détaillés au paragraphe 6.2 dans le cadre d'une étude comparative avec ceux offerts par FNBDT en référence à H.235.

Il est à noter que dans SRTP, les entêtes RTP sont envoyées en clair pour permettre la compression d'entête. Ce qui rend certains champs disponibles aux attaques (e.g. le payload, le SSRC et l'horodatage).

Le but de cette sécurité introduite par SRTP dans un contexte multimédia temps réel inclut la vitesse, le parallélisme, la non propagation des erreurs de bits et la limitation de l'expansion des paquets

Cependant SRTP présente quelques points faibles :

– SRTP n'adresse aucune sécurité de la signalisation. Ce qui requiert un mécanisme séparé pour tous les autres types de communications ;
– besoin d'une gestion de clé séparée, tel IKE, ISAKMP/Oakley, Kerberos ou de mécanismes de point à point tel Diffie-Hellman ;
– besoin de changer la programmation du protocole dans les téléphones IP ;
– manque d'authentification des utilisateurs dans des sessions RTP groupées ou multicast.

CHAPITRE 5

FUTURE NARROW BAND DIGITAL TERMINAL (FNBDT)

5.1 - Contexte historique

Dans les années 80, le STU-III (« *Secure Telephone Unit* ») constituait une solution matérielle nouvelle de sécurité pour les communications de voix et de données. En plus de sa petite taille d'équipement bureautique et d'un prix valant le quart de STU-II, son prédécesseur, le STU-III était le premier le téléphone sécurisé à offrir un choix du niveau de sécurité des communications de voix et de données. De 1987 à 1999, la *General Dynamics* a équipé les bureaux et salles de conférence de la Maison Blanche, du Pentagone et des différents entrepreneurs de défense de par le monde, de plus de 240 000 postes téléphoniques STU-III.

Au milieu des années 90, quatre niveaux distincts de sécurité avaient été définis pour les communautés d'utilisateurs spécifiques :

Type 1 : Le *Type 1* constitue le niveau le plus élevé de sécurité. Il a été exigé par le gouvernement américain pour la protection des informations classées Top Secret ;

Type 2 : La sécurité de *Type 2* a été prévue pour les informations sensibles mais non secrètes du gouvernement américain ;

Type 3 : La sécurité de *Type 3* a été conçue pour tous les autres besoins américains de sécurité domestique ;

Type 4 : La sécurité de *Type 4* a été définie pour la classe des produits sécurisés, à destination de clients internationaux.

Ces quatre groupes d'utilisateur pouvaient communiquer en toute sécurité au sein de leur communauté spécifique, mais ne pouvaient pas communiquer de façon sécurisée avec d'autres groupes d'utilisateurs. Par exemple, un utilisateur de *Type 1* ne pouvait pas avoir une conversation sécurisée avec un utilisateur de *Type 3* ou de *Type 4* parce que les produits sécurisés n'interopéraient pas.

Comme les affaires et les conditions géopolitiques ont changé, le gouvernement américain a éprouvé un besoin croissant d'intercommunication entre les différents niveaux de sécurité. D'autre part, comme les réseaux à fil, sans fil et ceux basés sur IP se développent d'une façon de plus en plus interopérable, la NSA (« *Nastional Security Agency* »), l'agence américaine en charge de la sécurisation des systèmes d'information, a lancé un certain nombre d'initiatives pour s'attaquer à jamais aux problèmes les plus durs de sécurité des réseaux, allant de l'interopérabilité d'Internet et la convergence des réseaux aux vulnérabilités des réseaux sans fil. Comme plus grand environnement non protégé d'interconnexion des réseaux sur le globe, l'Internet est un défi formidable de sécurité. Il représente aujourd'hui pour beaucoup le seul plus grand marché de sécurité.

En 1999, la NSA a réalisé une interopérabilité sécurisée entre les systèmes à fil (« *wire* ») et ceux sans fil (« *wireless* ») lorsqu'elle a créé un consortium industriel et gouvernemental qui a convenu d'un protocole commun de signalisation, appelé FNBDT (« *Future Narrow Band Digital Terminal* »), prononcez « Fend-Bid », qui a été également développé pour fournir un schéma de signalisation permettant aux utilisateurs de communiquer en toute sécurité avec d'autres produits compatibles.

Contrairement à ce que son nom l'indique, FNBDT n'est plus d'un ressort futur : en l'an 2000, alors que l'utilisation des réseaux sans fil pour les communications de voix et de données gagnaient déjà en popularité et en préférence, la filiale *General Dynamics Decision Systems* de *General Dynamics* a lancé *Sectéra*, une architecture de haute assurance d'interopérabilité sécurisée des réseaux de données et de télécommunications, dont les produits utilisent le plan de signalisation de FNBDT.

En début de l'année en cours (2004), le groupe de travail de FNBDT a augmenté le nombre de ses membres pour inclure la Grande-Bretagne, le Canada, l'Australie et la Nouvelle Zélande, aussi bien que l'OTAN dans un engagement séparé. Il a introduit FNBDT aux groupes de travail des normes de l'OTAN pour qu'ils l'étudient et le considèrent comme base pour l'interopérabilité sécurisée. Il espère ainsi se joindre à différentes nations pour concevoir un ensemble commercial de normes pour l'interopérabilité afin de s'assurer d'avoir en sa possession les bases de l'interopérabilité sécurisée avec ses alliés.

Il convient de noter que FNBDT a été offert aux nations de l'OTAN par les États-unis. Si les nations de l'OTAN décident d'adopter les protocoles de FNBDT, elles seront responsables des additions relatives à l'OTAN et/ou des extensions du standard. Les USA ont indiqué qu'ils travaillent actuellement sur les termes de référence pour un nouveau groupe mené par les USA qui accordera un forum pour les nations de l'OTAN afin qu'elles puissent participer plus tard au développement ou à l'extension des protocoles de FNBDT.

5.2 - Présentation générale

La définition de FNBDT représente une variation fondamentale dans le paradigme traditionnel de fragmentation. Au lieu de développer différents produits individuels de communications sécurisés, conçus pour interopérer entre eux, FNBDT définit une architecture interopérable et sécurisée indépendamment de la technologie du réseau sous-jacent.

FNBDT est une collection de protocoles interopérables permettant des communications de données et de la voix sans couture, sécurisées de bout-en-bout à travers une infrastructure hétérogène de réseaux. Le programme FNBDT est basé sur des normes et par conséquent construit sur des infrastructures d'investissement commercial (c.-à-d. PSTN, les réseaux RNIS et cellulaires, etc...) pour réaliser des produits et solutions de communications interopérables et sécurisés de bout-en-bout.

FNBDT est devenu la première norme de sécurisation des téléphones cellulaires, des radios militaires et de beaucoup de dispositifs publics de communications sécurisées émergents et destinés à servir des missions nationales de sécurité et de premiers répondeurs de par au monde.

FNBDT inclut des possibilités communes de traitement de la voix, un protocole de signalisation commun, une base commune d'algorithme cryptographique, et un processus commun de gestion de clés, chacun défini par un document différent :

- FNBDT-120 : Plan de Gestion des Clés ;
- FNBDT-210 : Plan de Signalisation (Version Formelle 1.1)
- FNBDT-230 : Caractéristiques Cryptographiques (sous forme d'ébauche – *draft*)
- FNBDT-220 : Conditions d'Interopérabilité (non officiel – *Informal*)
- FNBDT-6xx : Documentation d'Essai (discussion en suspens)

5.2.1 - Interopérabilité

FNBDT fournit l'interopérabilité par son matériel configurable par logiciel, une négociation commune de mode et de paramètres entre les terminaux pairs, et son indépendance totale du réseau sous-jacent, sinon la recommandation d'une largeur de bande minimale du canal sous-jacent de 2400 bps. FNBDT possède un ensemble commun de fonctions qui peuvent être soit fixées soit définies pour tous les terminaux à n'importe quelle moment. Ces fonctions sont utilisées par FNBDT pour la négociation de mode entre terminaux afin d'établir les modes de communication pour la connexion. L'interopérabilité entre les réseaux différents est réalisée par le fait que la norme ne définit pas les protocoles des couches inférieurs du réseau.

5.2.2 - Scénarios de communication de base entre un réseau SH et un réseau UN

Quatre scénarios de communication de base sont identifiés entre un réseau à système de sécurité élevé (*SH* pour « *System High* ») et un réseau non classifié (*UN* pour « *Unclassified* »). Une passerelle de confiance entre les deux réseaux, un élément essentiel dans une architecture de sécurité basée sur FNBDT, est supposée supporter FNBDT. Les terminaux FNBDT doivent pouvoir établir des connexions claires avec les terminaux non-FNBDT.

Le tableau ci-dessous montre l'état de la connexion résultante des quatre combinaisons possible entre un terminal supportant FNBDT et un non. La signalisation devrait être symétrique, c.-à-d. l'établissement et la fermeture d'appel peuvent provenir des deux terminaux. Les différents scénarios supposent que des connexions chiffrées d'une classification de sécurité supérieure et inférieure peuvent être établies dans le réseau *SH*. En outre on suppose que la passerelle a l'accréditation nécessaire pour le traitement de connexions pareilles, à plusieurs niveaux de sécurité.

Dans le dernier cas, n'importe quelle classification de sécurité permise entre les deux terminaux peut être négociée.

Terminal A	**Terminal B**	**Connexion**	**Remarque**
Non-FNBDT	Non-FNBDT	Le GW initie un NSW vers TE A	Seulement sur un réseau de voix
Non-FNBDT	FNBDT (*SH*)	TE A + tunnel *SH* entre GW et TE B	Indication d'une classification de sécurité à TE B
FNBDT (*SH*)	Non-FNBDT	Tunnel *UN* inverse entre TE A et la GW + connexion *UN* avec TE B	Indication d'une classification de sécurité *UN* à TE A.
FNBDT (*SH*)	FNBDT (*SH*)	Établissement d'un tunnel *SH* entre TE A et TE B	Indication d'une classification de sécurité aux TE

SH = System High UN = Unclassified TE = Terminal Equipment
GW = Gateway (passerelle) NSW = Non Secure Warning

Tableau 5.1 : *Ensemble des communications de base à travers une passerelle.*

5.2.3 - Objectifs de FNBDT

Un but majeur du programme FNBDT, est de minimiser l'investissement du gouvernement dans l'infrastructure de communications en exploitant l'évolution rapide de l'investissement commercial dans l'état de l'art de l'infrastructure COTS (Commercial-Off-The Shelf) (c.-à-d. cellulaire). Cette stratégie, associée aux protocoles communs FNBDT, a un avantage supplémentaire : celui de s'assurer que l'interopérabilité avec les systèmes de legs est maintenue.

FNBDT est capable de supporter plusieurs différentes communautés d'intérêt, qu'elles soient nationales, l'OTAN, ou des coalitions dynamiques. La ségrégation de ces communautés d'intérêt est rendue possible par l'utilisation de différents numéros d'identification de source (*source ID*) assignés aux groupes d'utilisateur. Des configurations nationales privées sont rendues possibles par le fait que quelque chose déclaré dans un domaine national d'identification de source n'a pas besoin d'être partagé avec d'autres nations. Ceci pourrait inclure une suite cryptographique, un formatage additionnel de protocole, des fonctions interagissant avec d'autres actifs de la communication nationale, etc. L'utilisation de l'approche prescrite par le programme de FNBDT résulte en l'élimination du besoin de multiples équipements indépendants pour les exigences de communications nationales, de l'OTAN et autres.

5.3 - Plan de gestion des clés

Pour établir un appel sécurisé, une nouvelle clé de chiffrage du trafic (***TEK*** – *Traffic Encryption Key*) doit être négociée. Pour la sécurité de *Type 1* (appels classifiés), le plan de signalisation FNBDT utilise pour l'échange de clé un système de transmission de messages augmenté de *FIREFLY*. *FIREFLY* est un système de gestion de clé développé par la NSA et basé sur la cryptographie à clé publique. Au moins une implémentation commerciale de qualité utilise l'échange de clé *Diffie-Hellman*.

À la différence de STU-III et de STE, qui utilisent des jetons de sécurité pour limiter l'utilisation des possibilités de voix sécurisée, aux utilisateurs autorisés, les téléphones FNBDT exigent seulement un code *PIN* (*Personal Identification Number*) de 7 chiffres pour la sécurité de *Type 1* et de 4 chiffres pour les appels non classifiés.

5.4 - Vue d'ensemble du plan de signalisation

La signalisation de FNBDT est initialement définie pour les terminaux qui opèrent au-dessus de canaux à bande numérique étroite tels que les cellulaires numériques commerciaux (CDMA de premier intérêt, GSM, TDMA, et plus tard d'autres), les satellite mobile (IRIDIUM™, Globalstar, ICO) et les canaux militaires et tactiques. Mais en dépit de son nom, la signalisation FNBDT est également compatible avec les canaux à large bande tels que l'Internet et l'ATM.

Le plan de signalisation de FNBDT utilise pour la définition de sa norme, les couches 5 (Session) et 6 (Présentation) de l'OSI (*Open Systems Interconnexion*) (cf. fig. 5.1). La couche Application contient des fonctions pour des services particuliers d'applications, tels que le transfert de fichier et l'accès à distance. Une application FNBDT utilise la technique de chiffrement Rijndael (connue aussi sous le nom de *Advanced Encryption Standard* (*AES*)) en mode compteur (*Counter-Mode*). FNBDT compte sur les développeurs d'applications pour spécifier les couches inférieures du réseau (couches OSI 1 à 4) afin de fournir la livraison de bout-en-bout des données.

En ne délimitant pas les couches du réseau, FNBDT fournit la plus grande flexibilité pour l'inclusion d'une variété de réseaux différents, et même des concaténations de réseaux différents. FNBDT utilise la signalisation de la couche application insérée dans la capacité de transport fiable de données fiables de n'importe quel point terminal de réseau. Cette signalisation de la couche application permet un format cohérent pour le trafic de voix et de données FNBDT couvrant les services support du transport par le biais de fonctions interagissantes (*IWF* pour « *Interworking Functions* ») qui permettent donc de traduire (ou connecter, interfacer) des données entre les réseaux donnés dans un scénario de réseaux hétérogènes.

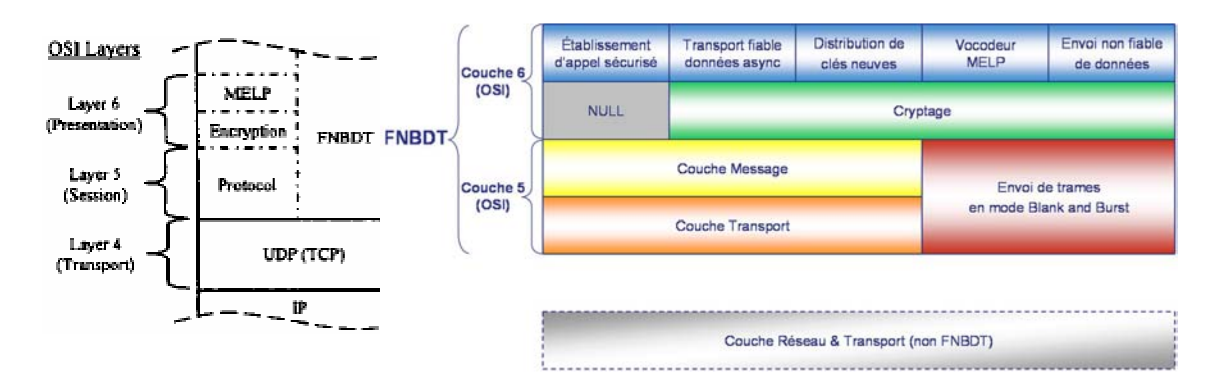


Figure 5.1 : *Les couches protocolaires de FNBDT.*

La figure 5.1 montre l'architecture de FNBDT. Les différentes couches et modes de fonctionnement sont définis, du bas vers le haut, comme suit :

- les couches physique, réseau et transport sous-jacents sont indépendants de FNBDT ;
- la couche *Transport* fournit un service de transport fiable pour les données avec accusé de réception. En d'autres termes, toute donnée perdue pendant la transmission devrait être renvoyée ;
- la couche *Message* permet de reconstruire les commandes issues de la couche application en des messages avant transmission à la couche en dessous. Elle s'occupe aussi de l'établissement et du contrôle d'appel ;
- la couche Blank & Burst permet l'envoi de trames de voix et de données sécurisées avec une tolérance des erreurs, des rejets et des évanouissements. Les données cryptographiques de synchronisation doivent être disponibles dans cette couche de façon fiable. Il n'y a pas d'espace pour la mise en trame et les retransmissions dans les données de voix. Le concept du système ne permet pas la mise en trame et les retransmissions des données cryptographiques de synchronisation. L'approche de gestion de synchronisation réalise la récupération de l'information de synchronisation en utilisant un vecteur d'état non classifié ;
- la couche *Cryptage* chiffre et déchiffre les données échangées ;
- le niveau le plus haut est composé de différents blocs d'application tels que l'établissement d'appel sécurisé, le transport fiable de données asynchrones, le renouvellement électronique des clés, le vocodeur MELP à 2400bps et les données asynchrones à débit garanti (c'est l'envoi non fiable de données).

La signalisation de FNBDT peut être transportée d'une manière transparente au-dessus d'un réseau de voix sur IP (VoIP). Des usagers d'un réseau sans fil sécurisé peuvent effectuer des appels non sécurisés sur un réseau VoIP. Ils peuvent également effectuer des appels sécurisés avec d'autres utilisateurs d'un réseau sans fil sécurisé ou avec les utilisateurs d'un terminal (par exemple, *STE*) qui supporte FNBDT.

Cependant, FNBDT est plus qu'un recouvrement, c'est « une prescription pour l'interopérabilité ». Le plan de signalisation FNBDT est structuré pour fournir les fonctions fondamentales nécessaires à l'établissement d'un appel sécurisé, l'échange des capacités, la négociation des paramètres de session, le changement de mode pendant un appel et la terminaison d'un appel.

Le plan de signalisation est prévu de façon flexible de sorte à s'adapter aux réseaux futurs et à des types de données additionnels.

En effet, les architectes du plan de signalisation de FNBDT ont standardisé des fonctions fondamentales pour tout équipement pouvant supporter FNBDT et ont réservé de l'espace protocolaire pour l'ajout en annexe d'aptitudes spécialisées et de services émergents.

Je signale que mon travail se base sur la spécification 1.1 de la signalisation FNBDT ; une nouvelle version pouvant apporter des modifications ou des améliorations. Dans cette version, le plan de signalisation définit :

i. l'échange des clefs, des certificats ou de toute autre information entre les deux terminaux en préparation à l'échange d'un trafic sécurisé de voix ou de données ;
ii. la transmission d'un trafic sécurisé de voix entre les terminaux des usagers pour des opérations point-à-point, utilisant le vocodeur standard du DoD (« *Department of Defense* »), le MELP (« *Mixed Excitation Linear Prediction* ») à 2400 bps ;
iii. la transmission d'un trafic sécurisé de données entre les terminaux des usagers pour une communication point-à-point de données sécurisée ;
iv. la signalisation de contrôle de la sécurité nécessaire pour établir, maintenir, et terminer le mode de fonctionnement sécurisé ;
v. les signalisations à définir plus tard pour supporter la réintroduction de clés de façon électronique ou *wireless* (*over-the-air*) ou les matériels de création de clés utilisés par les terminaux ;
vi. le point de signalisation de départ pour permettre aux fournisseurs d'ajouter des signalisations et des modes propriétaires définis par le reste du plan de signalisation.

5.4.1 - Exigences Essentielles Minimales (MER)

Le plan de signalisation définit plusieurs modes opératoires, pour chacun desquels la signalisation minimale doit être utilisée par les terminaux supportant FNBDT. Ceci inclut la signalisation pour les « fonctions du noyau de FNBDT », comme l'établissement d'appel sécurisée, qui est spécifiée dans le développement du plan de signalisation. Cependant, pas tous les terminaux capables de traiter FNBDT implémenteront tous les modes opératoires (par exemple, il y aura des terminaux seulement pour les données et d'autres seulement pour la voix).

Pour les données, FNBDT utilise un protocole de type *ARQ* (« *Automatic Repeat reQuest* ») avec *FEC* (« *Froward Error Correction* ») pour assurer une transmission fiable. Le récepteur accuse bonne réception des blocs de données et peut demander si nécessaire la retransmission d'un bloc.

Pour la voix, FNBDT envoie simplement une suite de blocs de données MELP pour maximiser l'utilisation de la bande passante disponible et cesse la transmission s'il n'y a aucune parole en entrée. Un bloc de synchronisation est envoyé environ 2 fois la seconde au lieu d'une trame de données. Les 14 bits de poids faible du compteur de chiffrement sont envoyés avec chaque bloc de synchronisation, ce qui suffit pour couvrir un évanouissement de plus de six minutes. Les parties restantes du vecteur d'état sont aussi envoyées de sorte qu'à la réception du troisième bloc de synchronisation, le vecteur d'état est entièrement récupéré. Ceci traite des évanouissements plus longs et permet à une station ayant la *TEK* (« *Traffic Encryption Key* ») appropriée de joindre un réseau et d'être synchronisée en moins de 1,5 secondes.

FNBDT peut fonctionner avec une variété de vocodeurs, mais la norme exige comme un minimum essentiel pour les services supports des communications de bout-en-bout et interopérables avec FNBDT, le support de MELP, avec des capacités additionnelles de synthétiseur pour une intelligibilité améliorée. MELP fonctionne à 2400 bps, émettant une trame de données de 54 bits toutes les 22,5 ms. (C'est le débit requis comme condition minimale pour la voix sécurisée afin de s'adapter à l'algorithme STANAG-4591 de codage de la voix). Le canal de données à 2400 bps peut être un canal synchrone avec exactement 2400 bps ou un canal asynchrone. Les spécifications du vocodeur MELP pour la voix (sécurisée et non sécurisée) à 2400 bps assurent donc l'interopérabilité des réseaux à large et étroite bande numérique, y compris les réseaux de legs.

Enfin, un autre point important est que toute application sécurisée, qu'elle soit de voix, de données ou de vidéo, peut être établie, aussi longtemps que les supports du réseau sous-jacent peuvent maintenir la bande passante.

5.4.2 - Diagramme d'état d'une application FNBDT

Figure 5.2 : *Diagramme d'état d'une application FNBDT – point-à-point*[1].

La figure 5.2 fournit un diagramme d'état d'une application de haut niveau conceptuel d'un terminal qui comporte la signalisation de FNBDT.

Le terminal démarre de l'état *Connection Terminated* dans lequel il n'y a aucun chemin de communication vers l'extrémité distante. Des interactions de la signalisation entre le terminal et le réseau est alors nécessaire pour établir un chemin de données clair, qui sera utilisé pour transmettre les messages FNBDT, et des modes natifs (non FNBDT) ont lieu au-dessous de la ligne. Les spécifications de FNBDT s'appliquent seulement à la signalisation qui a lieu au-dessus de la ligne, une fois qu'une liaison de données a été établie entre les deux extrémités.

L'état *Connection Idle* implique un canal de bout-en-bout de données non sécurisées (en clair), qui a été établi en étant capable de supporter au moins 2400 bps de données utiles, mais au-dessus duquel aucune signalisation d'une application FNBDT n'est en cours de traitement. Le MELP à 2400 bps est actuellement le seul standard FNBDT défini pour le mode de la voix en clair.

[1] LUCK Jay. Introduction to FNBDT Signaling, 2004.

Il est donc à bien noter que FNBDT offre aussi la possibilité d'une transmission de la voix en clair et que le choix du mode sécurisé nécessite pour toute opération l'échange d'une signalisation ; pour cela FNBDT requiert l'ouverture préalable d'un canal de données entre l'émetteur et le récepteur en mode natif (c.-à-d. non FNBDT).

Une fois dans l'état *Connection Idle*, des applications FNBDT peuvent être accédées et les terminaux effectuent le premier échange d'établissement d'appel FNBDT, le *Capabilities Exchange*, pour déterminer quelle application FNBDT (claire ou sécurisée) ou application propriétaire sera utilisée pour l'appel. Alors après un échange de capacités à travers les *Capabilities Exchange*, l'une ou l'autre de la signalisation standard de l'établissement d'appel FNBDT ou de la signalisation propriétaire, définie par le fabricant peut être utilisée. En plus de l'échange des capacités, d'autres échanges sont exigés pour négocier les paramètres pour des applications FNBDT sécurisées standard.

La fonction *Mode Change* permet un basculement entre des applications qui emploient la même clé de trafic ou entre des applications FNBDT non sécurisées. Les transitions à une fonction native commune, ou à des application utilisant des clés différentes, ou à d'autres applications, sont faites par un retour à l'état *Connection Idle*, initié par un message de notification, *Notification Message*. D'autres applications sécurisées (pas encore définies dans le plan de signalisation) pourraient être inclues, par exemple, des applications utilisant les suites cryptographiques internationales *AES*.

Pendant des périodes d'inactivité (*Idle Periods*), il n'y a aucune transmission de bits par l'application FNBDT, bien qu'il puisse y avoir des bits sur des liens individuels reliés au *handshaking* des protocoles du canal sous-jacent.

Pour terminer l'appel d'une application FNBDT standard, un message de notification (*Notification Message*) est utilisé pour retourner à l'état *Connection Idle* avec une indication que le mécanisme natif sous-jacent doit être utilisé pour fermer la liaison sous-jacente de données non sécurisées et retourner à l'état *Connection Idle*.

5.5 - Détails du plan de signalisation de FNBDT

5.5.1 - Transport des messages FNBDT

Les exigences nécessaires minimales pour le transport des messages FNBDT comprennent un nombre de mécanismes de contrôle d'erreur pour faciliter la livraison fiable des messages de signalisation au terminal distant. Les transmissions de la signalisation commencent par un fanion *Start Of Message* (*SOM*), se terminent par un fanion *End Of Message* (*EOM*) et seront dites dans ce rapport « groupes de trames ».

Un groupe de trame est composé de trames, chacune etant protegee par un code binaire *BCH* (*Bose-Chaudhuri, Hocquenghem (Error Correcting Code)*) utilisé pour les codes *FEC* (*Forward Error Correction*) et *CRC* (*Cyclic Redundancy Code*). Le recouvrement des erreurs de transmission qui ne peuvent être corrigées par le FEC est fourni à travers l'utilisation d'une combinaison d'acquittements positifs et de rejets sélectifs sur base du trame-par-trame. Un temporisateur de retransmission fournit une protection pour les cas où un groupe entier de trame est perdu ou n'arrive pas au terminal distant dans une forme reconnaissable. Finalement, une fonction de fenêtre coulissante, de 127 trames de largeur, est utilisée pour contrôler les transmissions.

5.5.1.1 - Limites horaires de transport des messages

Tout au long de ce document, l'on parle de trafic tramé (*framed*) et de trafic plein bande (*full bandwidth*). On désigne par « trafic tramé » un trafic formaté selon les informations de mise en trame introduites à la figure 5.3, commençant par un *SOM* et se terminant par un *EOM*. Par contre, un trafic *full bandwidth* fait référence à un trafic d'application transmis uniquement avec une information de gestion de synchronisation (*sync management information*). Il ne comporte alors pas d'en-tête *SOM* ni d'en-queue *EOM*, mais il se peut toutefois qu'il y ait d'autres couches de mise en trames fournies par le réseau sous-jacent. Un trafic *full bandwidth* est toujours précédé par une séquence *START*. Un temporisateur d'application est utilisé pour assurer la transition des deux terminaux communicants au trafic *full bandwidth*.

Il est aussi à noter que les canaux d'émission et de réception d'un terminal opèrent indépendamment. Cela veut dire que si un terminal reçoit un *START*, son canal de réception sera en trafic *full bandwidth*, mais son canal d'émission ne sera en trafic *full bandwidth* que lorsqu'il émettra un *START*. Il en résulte que durant les périodes de transition entre l'entrée et la sortie d'un trafic *full bandwidth*, un terminal peut en effet opérer avec les deux trafics : tramé et *full bandwidth*.

5.5.1.2 - Mise en trames de transport

La signalisation FNBDT peut être requise pour opérer au-dessus de canaux avec un taux d'erreur du bit de moins de 1%. Pour permettre un fonctionnement au-dessus de canaux pareil, les groupes de trames doivent être segmentés et formatés en des trames de 20 octets (cf. fig. 5.3) avant la transmission. Chaque trame doit contenir :
– un *FC* (*Frame Count*) de 1 octets ;
– 13 octets de données ;
– un *CRC* de 2 octets;
– une parité *FEC* de 4 octets.

Comme la figure 5.3 le montre, un groupe de trames commence par un *SOM* de 8 octets et se termine par un *EOM* de 8 octets. La taille de la trame est basée sur l'utilisation d'un code *BCH* abrégé (160, 128). Quand une transmission est reçue, chaque trame est décodée pour le FEC et le CRC est calculé pour déterminer si la trame contient des erreurs incorrigibles. Pour une retransmission, le même format est utilisé, sauf que seulement les trames demandées sont transmises.

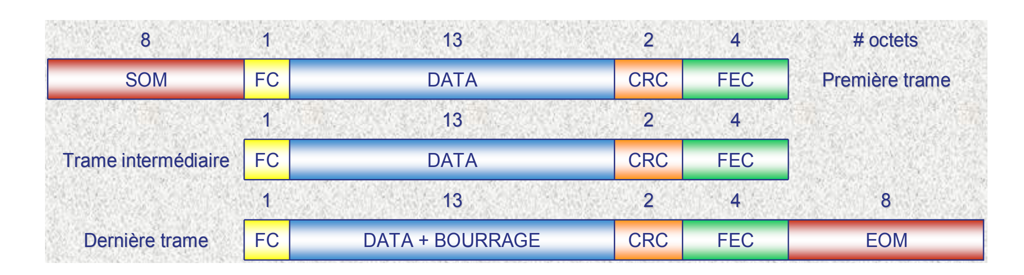


Figure 5.3 : *Groupe de trames à transmettre.*

i. SOM

Le *SOM* est une séquence pseudo-aléatoire de 64 bits qui précède chaque groupe de trame transmis. Il est conçu pour permettre une bonne performance de détection du groupe de trame dans des environnements qui prévoient des erreurs et pour permettre au récepteur de déterminer le premier bit du premier octet du groupe de trame afin de commencer le traitement.

ii. FC

Le *FC* permet aux trames d'être identifiées individuellement pour que seules les trames reçues avec des erreurs incorrigibles ont besoin d'être retransmises. Comme le montre la figure 5.3, le premier octet de chaque trame d'un groupe de trames transmis doit contenir le *FC*. Donc chaque message ou groupe de trames peut être formé d'au plus 255 trames, soit 253 trames intermédiaires. La première trame du premier message transmis, après une entrée initiale ou sur une réentrée du mode natif, doit avoir le *FC* = 0x01. Le *FC* doit être incrémenté pour chaque trame suivante transmise (modulo 256 – avec retour à 0x01 après 0xFF) sans souci des limites du groupe de trames. Le *FC* doit être aussi réinitialisé à 0x01 pour le premier groupe de trames suivant la transmission d'un *RESET*. Pour les messages de contrôle de la couche transport (*REPORT* et *RESET*), le *FC* doit être fixé à 0x00 pour toutes les trames. Ceci permet d'identifier les messages comme messages de contrôle de la couche transport.

iii. DATA

Les *DATA* occupent 13 octets par trame et peuvent être des type *Frames*, *REPORT* ou *RESET* ; les *Frames* étant les messages de données utiles. Il est à noter qu'un bourrage au niveau de la dernière trame s'avère souvent nécessaire pour compléter le format défini.

iv. CRC

Le *CRC* permet la détection d'erreurs résiduelles après que la correction d'erreur par le *FEC* ait eu lieu. Un *CRC* doit être calculé sur le *FC* et le champ *Data* de chaque trame. Le *CRC* doit être le standard nord américain *CRC-16*. Son générateur polynomial est : $P(x) = x^{16} + x^{15} + x^2 + 1$.

v. FEC

Le code *FEC* fournit la capacité de corriger les erreurs survenant pendant la transmission. Le *FEC* doit être implémenté avec quatre codes binaires de correction d'erreurs *BCH* abrégé d'un bloc naturel de taille 255 bits. La longueur du bloc du code est 160, il y a 128 bits d'information et 32 bits de vérification par bloc de code. Les bits de contrôle sont calculés sur les champs *FC, Data* et *CRC*, ce qui fait 128 bits d'information ou 16 octets. Son générateur polynomial est :

$$g(x) = x^{32} + x^{31} + x^{30} + x^{29} + x^{27} + x^{26} + x^{25} + x^{22} + x^{20} + x^{19} + x^{17} + x^{16} + x^{14} + x^9 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1.$$

vi. EOM

L'*EOM* est une séquence pseudo-aléatoire de 64 bits qui suit immédiatement la dernière trame de chaque groupe transmis de trames. Il permet au terminal récepteur de détecter de façon sûre la fin d'un groupe reçu de trames dans des environnements qui prévoient des erreurs. Il est à noter que l'*EOM* est le complément bit-à-bit *SOM*.

5.5.1.3 - La séquence ESCAPE

La séquence *ESCAPE* est une séquence pseudo-aléatoire de 32 octets qui permet une probabilité élevée de détection en arrière-plan de trafic *full bandwidth* sous le canal conditionné à cet effet. La séquence *ESCAPE* est utilisée pour permettre aussi la détection de groupes de trames transmis qui interrompent le trafic *full bandwidth*.

Quand un terminal transmet un trafic *full bandwidth*, il fera précéder les transmissions de groupes de trames par un *ESCAPE*. Le fait que le terminal récepteur distant est déjà entré en mode de trafic *full bandwidth* ou pas encore, n'est pas pertinent. S'il y est entré, la séquence *ESCAPE* est nécessaire et sera prise en considération. Sinon, elle sera ignorée et le *SOM* sera détecté.

Quand la transmission d'un groupe de trames, qui peut être soit un contrôle d'appel soit un message *REPORT*, est invoquée pendant une transmission *full bandwidth*, le terminal cesse de transmettre le trafic *full bandwidth*, transmet la séquence *ESCAPE* et permet la mise en trames. Le terminal composera et transmettra alors le groupe de trames demandé.

Un terminal qui reçoit une séquence *ESCAPE* pendant la réception d'un trafic *full bandwidth* permettra la réception d'un trafic tramé et traitera les groupes de trames entrants.

5.5.1.4 - Messages de contrôle de la couche transport

Les messages de contrôle de la couche transport sont des messages échangés entre des couches transport de pair et ne sont pas passés aux couches supérieures. Ils seront transmis avec le champ *FC* fixé à 0x00 pour les distinguer des messages destinés aux couches supérieures. Deux messages de contrôle de la couche transport sont définis pour la signalisation FNBDT. Il s'agit des messages *REPORT* et *RESET* ; chacun ayant une longueur d'une trame.

i. Le message REPORT



Figure 5.4 : *Format de la trame REPORT.*

Le message *REPORT* est identifié par la valeur 0x0020, qui est donc la valeur du champ *MID* (*Message IDentification*). Les champs *FC*, *CRC* et *FEC* étant communs à tous les types de trames, une trame *REPORT* est de 0x000B octets de long, mis à part les deux premiers et deux derniers champs du message ; c'est d'ailleurs la valeur du champ *Long*. Pour la version du message *REPORT*, définie dans la version 1.1 du plan de signalisation, la valeur du champ *Vers* est 0x00.

Le message *REPORT* est un message de rapport. Il sera donc transmis pour indiquer la réception réussie de trames contiguës d'un message et les trames perdues du message). D'où la nécessité des champs *AckFC* et *NackFC*.

Le champ *AckFC* contient le *FC* de la dernière des trames consécutives du message qui ont été reçues avec succès (c.-à-d. sans erreurs ou avec des erreurs corrigibles). Ceci dit, le *AckFC* indique que toutes les trames de la fenêtre envoyée jusqu'à, y compris la trame indiquée ont été bien reçues. Le terminal recevant le *REPORT* peut donc déplacer le début de sa fenêtre glissante de transmission jusqu'à la trame suivant celle dont le *FC* a été reportée dans le *AckFC*, libérant ainsi sa mémoire de toutes les trames qui ont été bien reçues. Il est à noter que les trames ne seront enlevées de la fenêtre de transmission qu'après avoir été acquittées et qu'au cas où la première trame du premier message suivant un message *RESET* ou sur entrée du mode natif est reçue erronée, le *AckFC* doit être mis à 255 (c.-à-d., à 0xFF).

La trame *REPORT* contient sept champs *NackFC* de un octet chacun. Ils servent de demande de retransmission au terminal distant des trames indiquées. Ils contiennent les *FC* correspondant à jusqu'à sept trames étant négativement acquittés (c.-à-d., indiquant que la trame n'a pas été reçue ou bien a été reçue mais avec des erreurs incorrigibles, détectées par l'échec du décodage du *FEC* et/ou de la vérification du *CRC*). Si moins de sept trames doivent être négativement acquittées, les champs *NackFC* restants inutilisés seront placés à 0x00. En outre, si plus de sept trames doivent être négativement acquittées, une ou plusieurs trames *REPORT* supplémentaires seront envoyées (par exemple, pour la demande de retransmission de 12 trames, 2 trames *REPORT* sont nécessaires.) Les *NackFC* inclus dans un message *REPORT* doivent l'être dans l'ordre croissant (avec 0xFF avant 0x01).

Sur ou après réception d'un ou plusieurs messages *REPORT* contenant des *NackFC*, un terminal composera un ou plusieurs groupes de trames, contenant seulement les trames indiquées dans les champs *NackFC* et les transmettra au terminal distant.

Un exemple d'utilisation des champs *AckFC* et *NackFC* est illustré à la figure 5.5 :

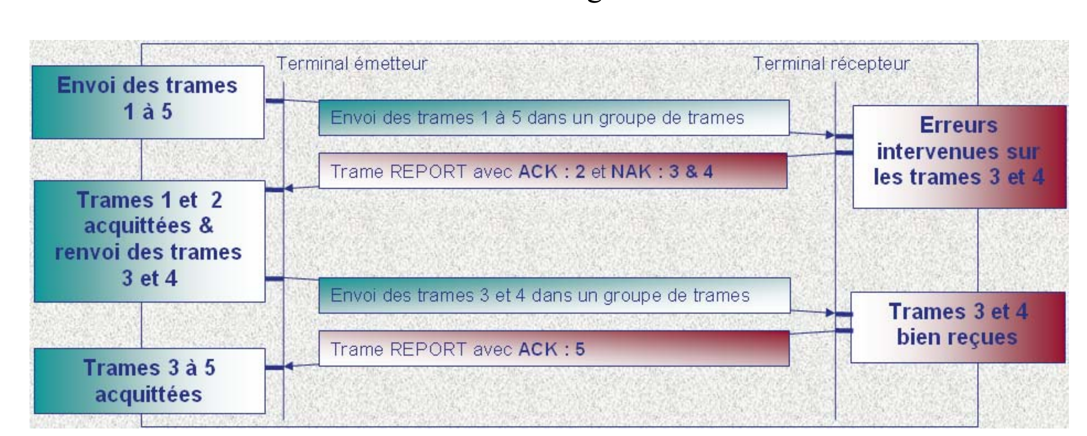


***Figure 5.5 :** Exemple d'utilisation des champs AckFC et NackFC.*

L'émetteur envoie un groupe de 5 trames. A la réception, le récepteur note qu'il lui faut une retransmission des trames 3 et 4 pour cause d'erreurs, il envoie alors à l'émetteur une trame *REPORT* avec *AckFC* = 2 et *NackFC* = 3 et 4. Le récepteur sait donc que les trames 1 et 2 ont été correctement reçues, décale sa fenêtre d'un pas de deux trames et renvoie les trames 3 et 4 dans un nouveau groupe de trames. Quand le récepteur les a bien reçues, il notifie l'émetteur par une trame *REPORT* avec *AckFC* = 5 et *NackFC* = 0. L'émetteur supprime alors de sa mémoire les trames 3 à 5.

ii. Le message RESET

Le message *RESET* sera utilisé pour resynchroniser la couche transport au besoin. Il peut également être utilisé pour « déblayer » le trafic en cours, soit donc pour réinitialiser le système, en cas de problèmes, par exemple. La transmission du trafic de la couche message cessera et tous les messages en cours seront rejetés. Les *FC*, pour des terminaux en appel point-à-point, seront réinitialisées à la valeur 0x01, de sorte que la prochaine trame attendue aura *FC* mis à 0x01.

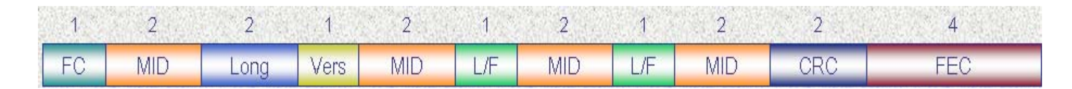


***Figure 5.6 :** Format de la trame RESET.*

Le message *RESET* est identifié par sa valeur du champ *MID*, fixée à 0x0080. Tout comme pour la trame *REPORT*, le champ *Long* de la trame *RESET* est fixé à 0x000B. De même, la version du message *RESET* est définie dans la version 1.1 du plan de signalisation à 0x00. Le fait que le champ *MID* est répété trois fois augmente la probabilité qu'il sera reconnu et utilisable dans le cas où il y a des erreurs résiduelles après le décodage du FEC.

Le champ *Leader/Follower* (*L/F*) se trouve deux fois dans la trame *RESET*. Il est mis à 0xFF pour les *RESET* transmis par le *RESET Leader* (le terminal qui transmet un message *RESET* en réponse à une indication locale) et il est mis à 0x00 pour les *RESET* transmis par le *RESET Follower* (le terminal qui répond à la réception d'un *RESET*). Un message *RESET* avec le champ *Leader/Follower* mis à 0xFF est désigné par *RESET(L)* et un message *RESET* avec le champ *Leader/Follower* mis à 0x00 est désigné par *RESET(F)*.

En réponse à une indication locale de *RESET*, un terminal (le *Leader*) cesse tous les messages et *REPORT* en cours et commence une transmission continue de *RESET(L)*.

À la réception d'un *RESET(L)*, un terminal (le *Follower*) cesse tous les messages et *REPORT* en cours et commence une transmission continue de *RESET(L)*. Il est à noter qu'à la réception d'un *RESET(L)* indiquant que les deux terminaux fonctionnent comme *Leader*, le terminal cesse de transmettre des *RESET(L)* et procède comme *Follower*. Donc, si les deux terminaux démarrent comme *Leader*, ils vont d'habitude tous les deux devenir des *Follower*.

À la réception d'un *RESET(F)*, un terminal *Leader* cesse d'envoyer des *RESET(L)* et reprend la transmission d'un trafic tramé, de couche message. Après une période de temps où aucun *RESET(L)* n'est reçu ou bien après la réception d'un groupe de trames valide et qui n'est pas un *RESET*, un terminal *Follower* cesse d'envoyer des *RESET* et revient à une transmission d'un trafic tramé, de couche message et le temporisateur de fin du *RESET* est arrêté. Il est à noter qu'aucun trafic de couche message n'est transmis quand le terminal est en train de transmettre des *RESET*.

Un exemple de transmission de *RESET* est illustré à la figure 5.7 :

Figure 5.7 : *Exemple de transmission de RESET.*

5.5.1.5 - Transmission des messages

Une fenêtre glissante de taille 27 est utilisée, c.-à-d., jusqu'à 127 trames non acquittées peuvent être en suspens. Pendant une opération de *RESET*, le processus décrit dans cette section aura déjà cessé et sera repris à l'accomplissement de l'opération *RESET*.

Quand les deux terminaux attendent une transmission, les messages *REPORT* doivent être transmis avant les messages reçus des couches supérieures. Ces derniers seront transmis dans l'ordre selon lequel les demandes de transmission ont été faites.

Quand la transmission d'un message est demandée par les couches supérieures, la fonction de transmission de message vérifie pour voir s'il y a de la place dans la fenêtre. La fenêtre est pleine si la différence entre le *FC* de la prochaine trame à transmettre et le *FC* de la dernière trame acquittée, donc si la différence de ces deux *FC*, modulo 255, vaut 128. Cependant, les messages *REPORT* peuvent être transmis même si la fenêtre est pleine. Donc si la fenêtre est pleine et que le message n'est pas un *REPORT*, il est retenu. Si la fenêtre n'est pas pleine ou si le message est un *REPORT*, un groupe de trames est transmis. Dans le cas où le message en cours de transmission n'est pas un *REPORT*, le groupe de trames peut contenir jusqu'à autant de trames qu'il y a de place dans la fenêtre ; le reste du message sera retenu. Si la fenêtre est pleine, le message retenu (ou la partie retenue d'un message partiellement transmis) sera transmis quand la fenêtre ne sera plus pleine.

Un *SOM* est transmis d'abord. Puis, si la contrainte de fenêtre le permet, toutes les trames de message sont transmises, suivies par l'*EOM*. Si le message entier ne peut être contenu dans la fenêtre courante, la partie non transmise du message est maintenue et sera transmise quand la fenêtre n'est plus pleine. Quand la transmission de trames est arrêtée à cause d'une fenêtre pleine, la dernière trame transmise sera suivie d'un *EOM*. La prochaine transmission commencera alors par un *SOM*. Immédiatement après la transmission de l'*EOM* du groupe de trames, à moins que le message n'ait été un *REPORT*, le temporisateur de retransmission sera (ré)initialisé à sa valeur initiale et (re)lancé de sorte que les trames puissent être retransmises si aucun *REPORT* n'est reçu.

Si la transmission se suit une séquence *START* transmise (c.-à-d., pendant un trafic *full bandwidth*), le groupe de trames sera précédé par une séquence *ESCAPE*.

i. Temporisateur de retransmission

En plus de la retransmission des trames acquittées négativement, les trames non acquittées sont retransmises à l'expiration du temporisateur de retransmission.

Le temporisateur de retransmission est (re)lancé à la transmission initiale et à chaque retransmission. À son expiration, les trames précédemment transmises et pas encore acquittées seront mises en un nouveau groupe de trames et retransmises. Si un ou plusieurs groupes de trames précédents étaient transmis, précédés par une séquence *ESCAPE* et aucun *REPORT* n'a été reçu depuis pour les trames de ce ou ces groupes, la retransmission sera précédée par une séquence *ESCAPE*.

5.5.1.6 - *Réception des messages*

Quand le *SOM* est reçu, le récepteur analysera une trame de 20 octets du flux de données entrant. Il peut exécuter un décodage *FEC* et utilisera le *CRC* pour vérifier que la trame a été correctement reçue ou que des erreurs de transmission ont été corrigées pendant le décodage *FEC*.

Si le *CRC* est subi avec succès et que le *FC* n'est pas à zéro (c.-à-d., le message n'est pas un message de contrôle de la couche transport) et se trouve dans est la fenêtre de réception attendue, la trame sera marquée comme correctement reçue. Les trames en dehors de la fenêtre de réception attendue seront rejetées sans traitement additionnel. La fenêtre de réception glisse et s'étend alors de la trame suivant le *AckFC* courant, c.-à-d., la trame suivant la dernière trame reçue et acquittée, jusqu'à 127 trames après le *AckFC*.

Si le test du *CRC* passe et que le *FC* est à zéro (c.-à-d., le message est un message de contrôle de la couche transport), le terminal déterminera si un *REPORT* ou une *RESET* a été reçu. Chaque type de message est identifié par son *MID*.

Si ni un *REPORT* ni un *RESET* n'a été reçu, aussi si la vérification par *CRC* ne passe pas, les octets suivants reçus sont examinés pour identifier un *EOM*.

Si ni un *EOM* ni un autre *SOM* ne suit, le récepteur analysera la prochaine trame de 20 octets et répétera le traitement ci-dessus.

Le récepteur répétera le processus ci-dessus jusqu'à réception soit du *EOM*, soit du prochain *SOM*. À la réception du *EOM* ou du prochain *SOM*, le terminal composera et transmettra un *REPORT*. Plusieurs *REPORT* peuvent être utilisés, puisque chaque *REPORT* peut identifier seulement sept trames acquittées négativement.

Si un *EOM* est reçu, le récepteur attend le prochain *SOM*. Si un *SOM* est reçu, le récepteur débute immédiatement le traitement des trames qui suivent le *SOM*.

5.5.2 - Signalisation d'établissement d'appel FNBDT

Une application suivant le plan de signalisation FNBDT doit d'abord exécuter son propre établissement d'appel en établissant de bout-en-bout une connexion native de données, utilisant pour cela les protocoles de communication réseau des couches inférieures (TCP, UDP, RTP, etc.). Une fois le canal natif de données est établi bout-en-bout, le contrôle (du canal) est passé à FNBDT qui procède alors à l'exécution de la signalisation de ses couches supérieures pour établir une session FNBDT point-à-point. Le réseau de communication apparaît donc comme un simple « tuyau » de données pour FNBDT.

Pour assurer l'échange réussi des données de contrôle et de signalisation, FNBDT utilise un transport fiable de messages qui utilise plusieurs mécanismes de contrôle d'erreur, qui incluent la mise en trames, le *FEC*, le *CRC*, les retransmissions et une combinaison d'acquittements positifs et de rejets sélectifs.

Avant le transfert sécurisé (ou en clair) de voix ou de données, les deux terminaux FNBDT initialisent une signalisation d'établissement d'appel point-à-point qui inclut la négociation, la sécurité, et le contrôle. Un message *Capabilities Exchange* est suivi par des messages *Parameters/Certificate*, des messages *F(R)* (*Forward and Reverse*) et des messages *Cryptosync*. Les messages *Capabilities Exchange* sont utilisés pour négocier le mode opérationnel (et choisir un ensemble de clés (*Keyset*)) communs aux deux terminaux. Si les deux terminaux ont convenu d'un mode opérationnel *en clair*, la signalisation d'application en clair commence. Si les deux terminaux ont convenu d'un mode opérationnel *sécurisé*, l'établissement d'appel procède par l'échange des messages *Parameters/Certificates* et *F(R)*. À la réception de ces messages, les terminaux utilisent le *Certificat* et le *F(R)* pour l'ensemble de clés choisi pour générer une clé de trafic commune. Les terminaux vont alors coder et chiffrer un ensemble commun de données, échanger les données chiffrées en les plaçant dans les messages *Cryptographic Exchange*. Pendant l'échange des messages de signalisation ci-dessus, des rapports sont envoyés entre les terminaux d'extrémité. Les rapports indiquent la réception avec ou sans succès des messages. Une fois la signalisation est achevée, les terminaux procèdent au transfert de données selon le mode opérationnel choisi.

Si un terminal reçoit le message du terminal distant avant de transmettre son propre message, il peut commencer à traiter le message reçu, parallèlement à la génération de son propre message tant que ceci ne retarde pas la transmission de ce dernier.

La figure 5.8 illustre les phases d'établissement d'appel FNBDT sécurisé.

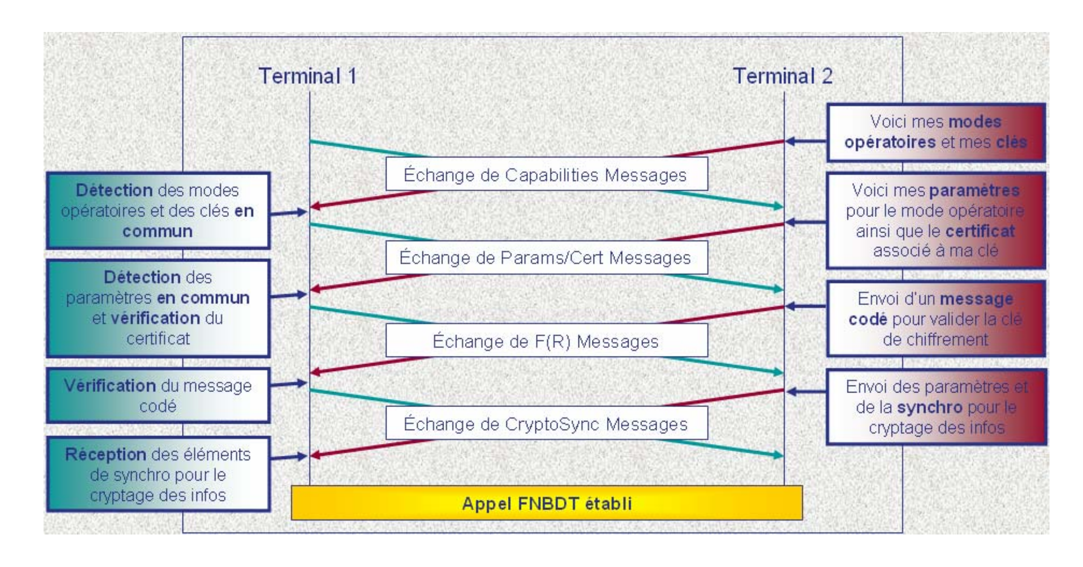


Figure 5.8 : *Phases d'établissement d'appel FNBDT sécurisé.*

La figure 5.9 montre les différents messages dans leur ordre d'émission pour l'établissement d'appel FNBDT sécurisé.

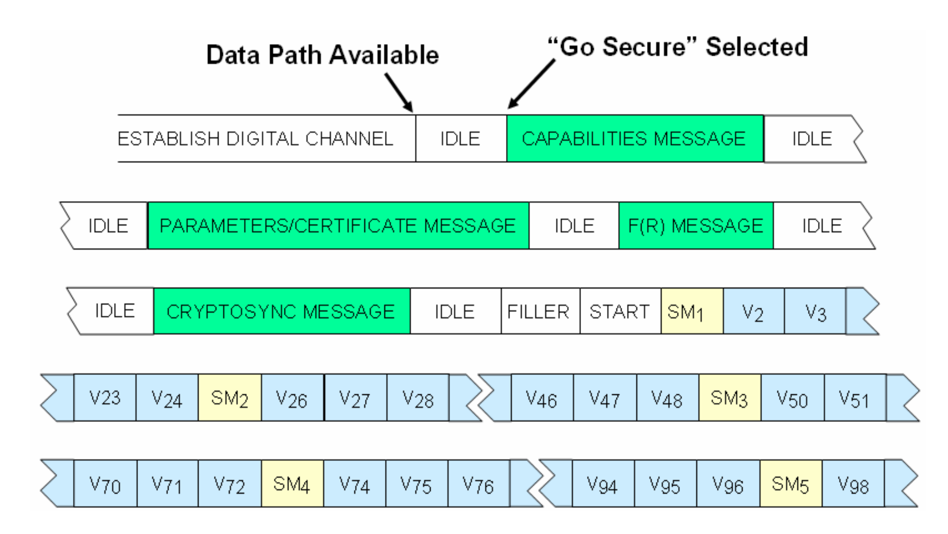


Figure 5.9 : *Séquence des messages d'établissement d'appel FNBDT sécurisé.*

5.5.2.1 - Le message Capabilities Exchange

La première étape dans l'établissement d'un appel FNBDT est l'échange des messages *Capabilities*. Cet échange permet aux terminaux de négocier un mode opérationnel en clair ou sécurisé que tous les deux soutiennent. Pour des modes opérationnels sécurisés, il permet également aux terminaux de choisir des ensembles de clés compatibles pour lesquels des créances seront plus tard échangées.

À partir de l'état *Connection Idle* et sur une demande locale d'entrée en un mode opérationnel, qui peut être automatique ou manuelle (par exemple, l'appui d'un bouton sur la console), un terminal commence comme initiateur, compose un message *Capabilities* et le transmet au terminal distant. Puisqu'en ce moment, pendant l'établissement initial de la connexion, le terminal ne sait pas encore qu'il y a à l'autre extrémité un autre terminal compatible avec FNBDT, il arme un temporisateur *de premier message* et attend un message *Capabilities* de l'extrémité distante. Le temporisateur *de premier message* expire si l'initiateur ne reçoit pas une réponse reconnaissable de l'extrémité distante.

La signalisation de répondeur diffère de celle de l'initiateur seulement par le fait qu'elle est initiée à la réception d'un message *Capabilities* de l'extrémité distante et que le bit d'ordre supérieur du champ de négociation de l'initiateur (*Initiator Negociation* ; cf. fig. 5.10) est mis à 0.

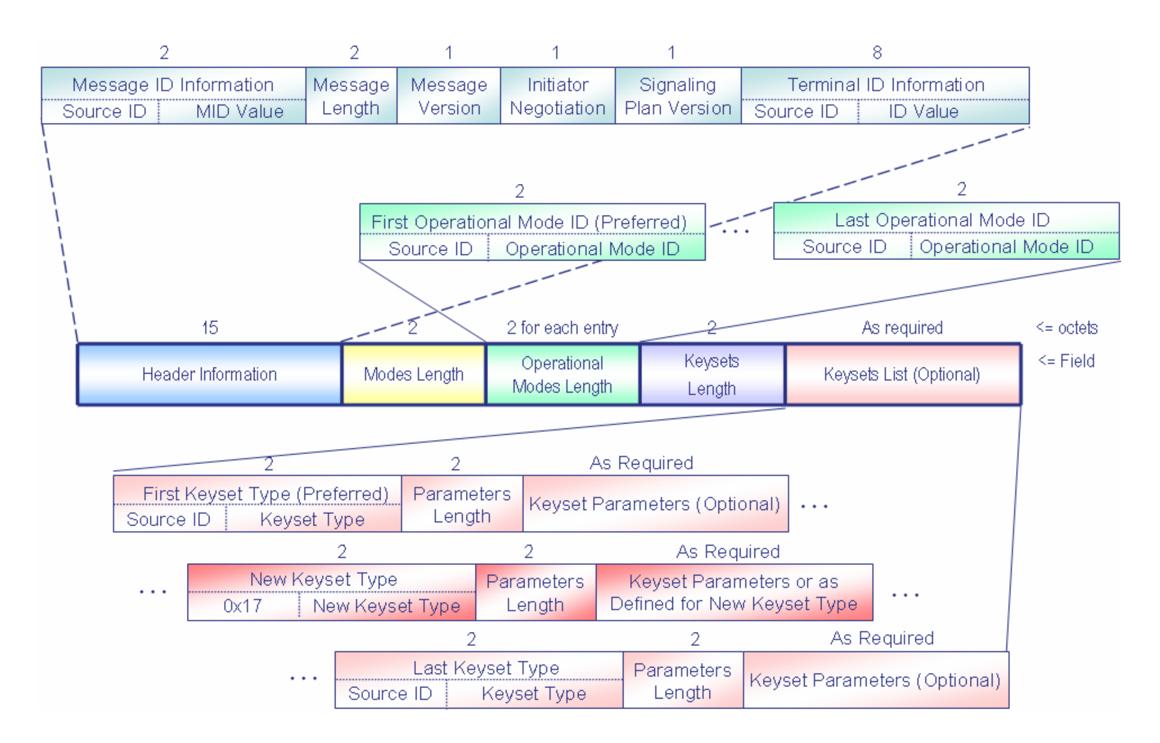


Figure 5.10 : *Format du message Capabilities.*

Un message *Capabilities* peut également être reçu soit quand les capacités reçues doivent être réexaminées parce qu'un échange de *Parameters/Certificate* a déterminé que des paramètres compatibles n'existent pas pour le mode opérationnel choisi, soit quand un des certificats échangés s'avère avoir expiré.

À la réception d'un message *Capabilities*, le terminal arrête le temporisateur *de premier message* puisqu'il sait maintenant que le terminal distant est compatible avec FNBDT.

Pour tout mode opérationnel sécurisé à choisir, des ensembles de clés compatibles l'un avec l'autre et avec le mode opérationnel, existent dans les listes *Keyset Parameter* des deux terminaux.

S'il n'y a aucun mode opérationnel commun ou aucun mode opérationnel commun suivant sur la liste de l'initiateur conforme au processus, le terminal exécute une logique de *Failed Call* avec un code d'information *no common operational modes*.

Si un mode opérationnel sécurisé standard a été choisi, il sera choisi un ensemble de clés compatible avec ce mode opérationnel et avec un ensemble de clés de l'autre terminal.

Si un mode opérationnel sécurisé était le premier choix du terminal mais un mode opérationnel *en clair* a été choisi, le terminal inciterait l'utilisateur et attendrait un acquittement avant entrée dans le mode *en clair*. Si le mode *Clear MELP Digital Voice* de FNBDT a été choisi, le terminal lance l'application *Clear MELP Digital Voice* de FNBDT. Si un mode d'opération en clair mais natif a été choisi, le terminal termine la signalisation FNBDT et revient à l'état *Connection Idle* à partir d'où le terminal peut exécuter la signalisation native indigène nécessaire pour appeler le mode opérationnel *en clair* choisi.

5.5.2.2 - Le message Parameters/Certificate

Si un mode opérationnel sécurisé est choisi, la deuxième étape de l'établissement d'appel FNBDT est l'échange des créances qui seront employées pour générer la clé de trafic. Les créances du *SDNS* (*Secure Data Network System*) actuellement utilisées par la signalisation FNBDT sont formées de deux parties, un certificat et un *F(R)*, qui sont échangés dans des messages séparés. À ce moment sont également négociés tous les paramètres qui doivent l'être pour le mode opérationnel sécurisé choisi. Si un mode opérationnel de voix *en clair* est choisi, il n'y a pas d'échange de créances.

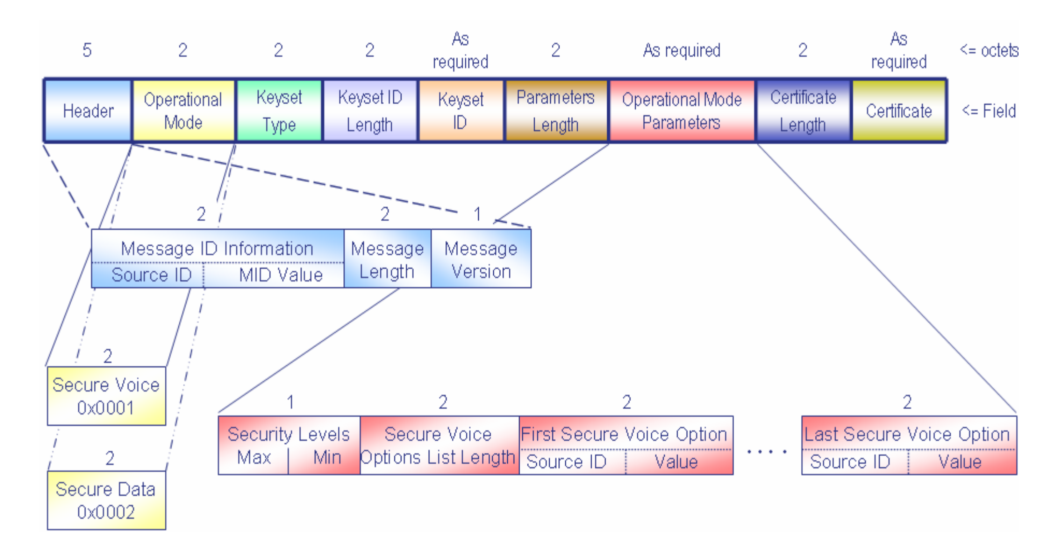


Figure 5.11 : *Format du message Parameters/Certificate.*

Les paramètres pour le mode opérationnel choisi et ceux pour le certificat de l'ensemble des clés seront tous transmis dans un message *Parameters/Certificate*.

Le terminal peut commencer à traiter dès réception le message *Parameter/Certificate* en provenance du terminal distant, pour le mode opérationnel et l'ensemble des clés choisis. Les entrées des listes des paramètres du mode opérationnel sont vérifiées. La première entrée de la liste des options rencontrée dans la liste des paramètres du mode opérationnel de l'initiateur et qui est supportée par le répondeur sera choisie.

Si aucune entrée de liste d'options sur la liste de l'initiateur n'est supportée par le répondeur, ou si pour les données sécurisées de *Type 1* ou la voix sécurisée de *Type 1* il n'y a aucun niveau de sécurité soutenu par les deux terminaux, le mode opérationnel est considéré incompatible et n'est pas à choisir.

Si le terminal a une *CKL* (*Compromised Key List*), le terminal doit d'abord comparer la date d'échéance du certificat à la date d'arrêt de la clé (*Key Cutoff Date*) dans le *CKL*. Si la date d'échéance dans le certificat est plus tôt que la *Key Cutoff Date* dans le CKL, le terminal affichera un message à l'utilisateur, signalant que le certificat reçu a expiré et risque d'être compromis. Sinon, le terminal comparera alors la date d'échéance dans le certificat à l'horloge de confiance ou la date (mois/année) d'origine du *CKL*. Si la date d'échéance dans le certificat est plus tôt, le terminal a borne affichera un message à l'utilisateur, signalant que le certificat reçu a expiré.

Si le certificat a expiré, le terminal attend alors l'Ok de l'utilisateur avant de procéder. Si l'Ok de l'utilisateur est en marche, alors les terminaux essaieront de choisir un ensemble de clés et/ou un autre mode opérationnel différents. (Évidement, l'utilisateur a toujours le choix de terminer l'appel téléphonique, et si l'option est soutenue, de passer en mode non sécurisé.)

5.5.2.3 - Le message F(R)

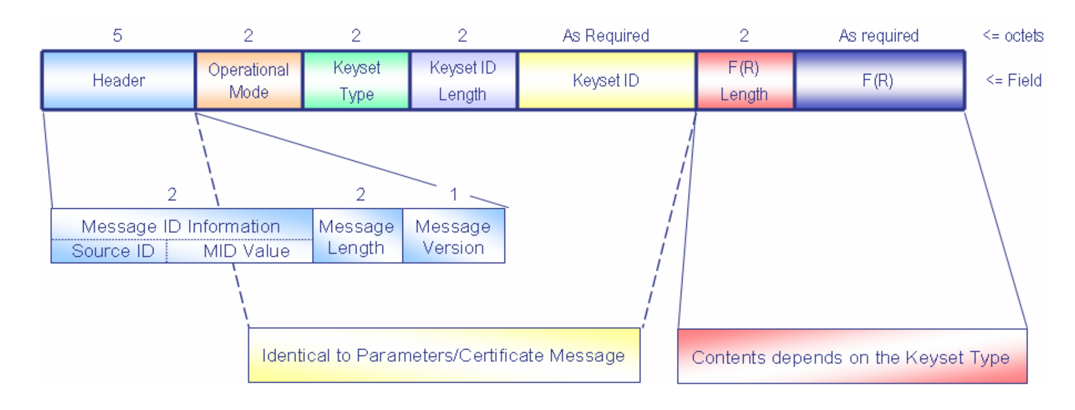


Figure 5.12 : *Format du message F(R).*

À cet instant, du côté de l'émission, le message *Parameters/Certificate* a été déjà composé et transmis. Un message *F(R)* contenant le *F(R)* pour l'ensemble des clés choisi est transmis à l'extrémité distante.

Du côté de la réception, le terminal a à cet instant déjà traité le message *Parameters/Certificate* reçu pour le mode opérationnel choisi et a déterminé que le mode opérationnel et ses paramètres, ainsi que le certificat, sont acceptables. Le terminal peut alors commencer à traiter les *F(R)* provenant du terminal distant, pour le mode opérationnel et l'ensemble des clés choisis, dès leur réception.

5.5.2.4 - Le message Cryptosync

La troisième étape dans l'établissement d'appel FNBDT est l'échange des messages *Cryptosync*. Les *IV* (*Initialization Vectors*) de l'application sont échangés ainsi que les données chiffrées qui permettent au récepteur de vérifier que le chiffrage disponible le plus sécurisé a été négocié et qu'il fonctionne correctement.

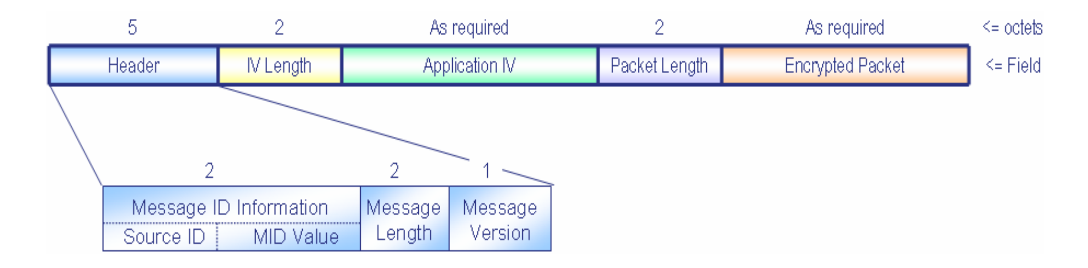


Figure 5.13 : *Format du message Cryptosync.*

À cette étape, pendant l'établissement d'appel FNBDT, les créances du terminal ont déjà été transmises et celles du terminal distant ont déjà été reçues et traitées. La génération de clé est en cours.

Quand le terminal a la clé générée, il formate les données à vérifier. Ces données seront chiffrées en utilisant un algorithme et un mode cryptographiques.

Pour l'ensemble choisi de clés *SDNS*, si la version de CKL dans le message *Capabilities* reçu de possibilités est avant la version locale du CKL, le terminal attend jusqu'à réception d'un message *Cryptosync* de l'extrémité distante. Autrement, le terminal transmet un message *Cryptosync* à l'extrémité distante et attend jusqu'à en recevoir un message *Cryptosync*. Dans les deux cas, le terminal traite le message *Cryptosync* provenant du terminal distant dès qu'il le reçoit. Il vérifie le paquet chiffré contenu dans le message *Cryptosync*. Si ce contrôle n'est pas réussi, le terminal exécute une logique de *Failed Call* avec un code d'information *no common operational modes*.

5.5.3 - Signalisation de contrôle d'appel FNBDT

Une fois invoqué, par une indication interne ou par une demande initiée par l'utilisateur, le terminal exécute la signalisation de contrôle d'appel pour exécuter des fonctions telles que la terminaison d'un appel, le changement de l'application, l'alerte du terminal distant et la resynchronisation cryptographique.

La signalisation de contrôle d'appel nécessite quatre messages différents : *Notification*, *Mode Change Request*, *Mode Change Response* et *Cryptosync*. Ils sont envoyés en mode de trafic tramé et peuvent interrompre le trafic *full bandwidth*.

5.5.3.1 - Le message Notification

Le message *Notification* remplit plusieurs fonctions et a six actions associées à l'exécution de ces fonctions : *Connection Terminate*, *Native Clear Voice*, *Connection Idle*, *CKL Transfer*, *Secure Dial* et *Attention*.

Les messages *Notification* contenant n'importe laquelle de ces actions sont envoyés *en clair* et peuvent l'être à tout moment, sauf pour *Secure Dial*. Puisque l'envoi de *Secure Dial* exige d'avoir une clé négociée et vérifiée, il peut être envoyé seulement après échange et vérification de messages *Cryptosync*. Un terminal invoqué pour exécuter une de ces fonctions produit une indication locale pour qu'un message *Notification* soit composé et envoyé à l'extrémité distante.

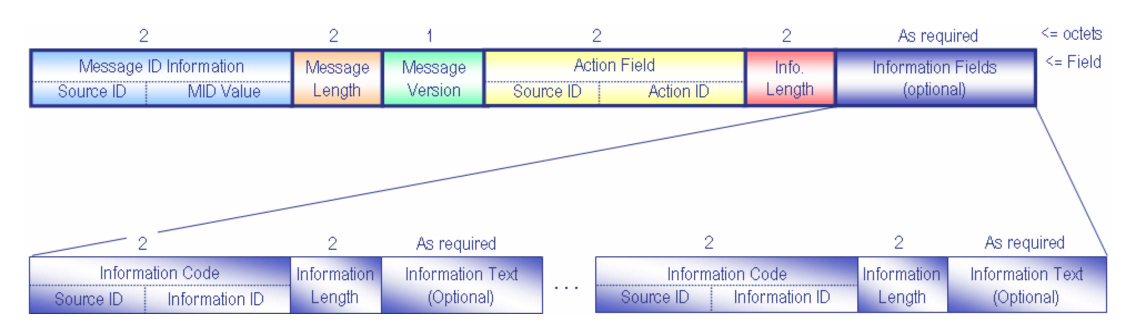


Figure 5.14 : *Format du message Notification.*

Un message *Notification*, avec l'action *Connection Terminate*, *Native Clear Voice* ou *Connection Idle* a une priorité plus élevée et à sa réception, il interrompt tous les messages restants de contrôle d'appel et *Notification* avis d'autres actions, qui sont tous traités sur base de *FCFS* (*First Come First Served*).

5.5.3.2 - Les messages de changement de mode

Les messages *Mode Change Request* et *Mode Change Response* sont impliqués dans le traitement de changement de mode qui sera entrepris seulement quand les deux terminaux sont dans un trafic d'application sécurisé. L'utilisation du changement de mode sera limitée à un changement d'une application sécurisée à une application sécurisée différente utilisant la même clé.

5.5.3.3 - Le message Cryptosync

Seulement le message *Cryptosync* est impliqué dans le procédé de resynchronisation bidirectionnelle (*Two-Way Resync*) qui est invoqué quand un terminal dans un trafic d'application sécurisé reçoit une indication locale de resynchronisation bidirectionnelle, qui est générée quand un terminal détecte qu'il est devenu *cryptographiquement* hors de synchronisation avec l'extrémité distante.

5.6 - Signalisation d'application d'utilisateur de FNBDT

Pour transférer des données sécurisées et des données *en clair*, FNBDT définit une variété de modes qui incluent éventuellement des sources multimédia. Cinq applications d'utilisateur sont actuellement définit :

i. *Secure 2400 bps MELP Voice – Blank and Burst* ;
ii. *Secure MELP Voice – Burst without Blank* ;
iii. *Clear 2400 bps MELP Voice* ;
iv. *Secure Reliable Transport (RT) Asynchronous Data* ;
v. *Secure 2400 bps Guaranteed Throughput (GT) Asynchronous Data*.

Les divers modes de communication décrivent le formatage du flux de données – dans ce cas-ci le flux de paquets. Chaque mode utilise une structure de supertrame qui entraîne le placement d'une trame de gestion de synchronisation (*Sync Management*) de 54 bits suivie d'un certain nombre de trames de voix.

La voix MELP et les applications *GT Asynchronous Data* sont des applications *full bandwidth*, puisqu'elles sont conçues pour usage sur des connexions où le taux d'information est égal, ou approximativement égal, au taux disponible du canal.

Des applications définies en tant que transport fiable (par exemple, *Secure RT Asynchronous Data*) sont exigées pour maintenir la fonctionnalité de la couche *Transport* après exécution de la signalisation d'établissement d'appel ou de changement de mode. Il est à noter que les applications *full bandwidth* sont exigées pour dévier la fonctionnalité de la couche *Transport* quand elles sont invoquées.

5.6.1 - MELP

MELP a été développé par Texas Instruments en tant qu'élément du *Defense Digital Voice Processor Consortium* (*DDVPC*), plus particulièrement en tant que candidat pour devenir un nouveau codeur standard de la parole à 2400 bps. MELP est actuellement proposé pour devenir une nouvelle norme fédérale pour une haute qualité de la parole à 2400 bps, remplaçant les normes fédérales FS-1015 (LPC-10) et FS-1016 (CELP), qui, par les normes modernes, produisent une parole de basse qualité. MELP à 2400 bps fonctionne aussi bien voire mieux que la norme fédérale FS-1016 (CELP) à 4800 bps, qui est le système de repère courant pour la parole à bas débit, ce qui fait de MELP un excellent candidat pour la parole à bas débit et un excellent candidat pour les applications de voix sécurisée à bas débit pour le gouvernement et les militaires.

Avec des échantillons de parole à 8000 Hz, MELP opère sur des trames de la parole de 22,5ms, produisant des trames codées et empaquetées de 54 bits chacune. Pour les 2400 bps de débit désiré, le taux résultant des trames est approximativement 44 trames par seconde.

5.6.2 - Voix MELP sécurisée

Dans le mode MELP de voix sécurisée, la trame *Sync Management* contient de l'information qui permet aussi bien la synchronisation cryptographique que son entretien pour les données de la supertrame correspondante. Trois des modes de communications possibles sont :

– *Clear 2400 bps MELP Voice* ;
– *Secure 2400 bps MELP Voice – Blank and Burst* ;
– *Secure MELP Voice – Burst without Blank.*

5.6.2.1 - Clear 2400 bps MELP Voice

Clear 2400 bps MELP est un mode de voix brute qui inclut une trame *Sync Management* de 54 bits suivie de 23 trames de voix MELP. La trame *Sync Management* remplace la première trame de voix MELP dans la structure de la supertrame, n'ajoutant aucune surcharge additionnelle au de flux de données à 2400 bps. Au récepteur, la trame de voix manquante doit être compensée par l'utilisation d'une stratégie de remplacement de trame à la réception de la supertrame.

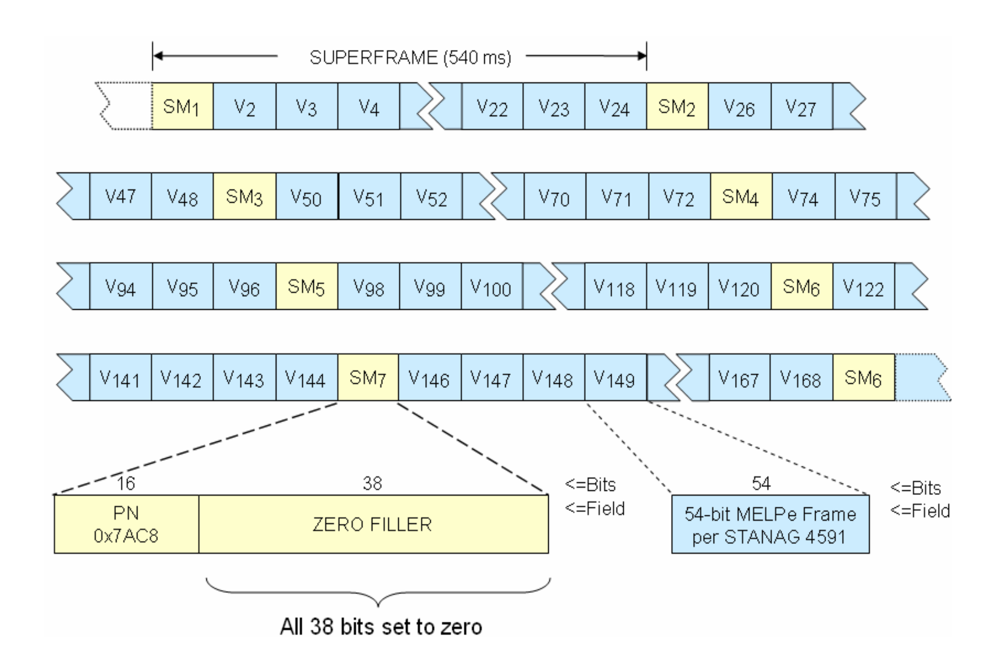


Figure 5.15 : *Clear 2400 bps MELP Voice – Format de transmission.*

5.6.2.2 - *Secure 2400 bps MELP Voice – Blank and Burst*

Dans le mode *Blank and Burst* du *Secure 2400 bps MELP*, excepté pour la première supertrame suivant un gap dans la parole, la première trame de voix MELP d'une superframe est jetée et remplacée par une trame *Sync Management* de 54 bits d'une manière similaire au mode MELP *en clair*. Ainsi, la supertrame *Blank and Burst* est de 24 trames de long.

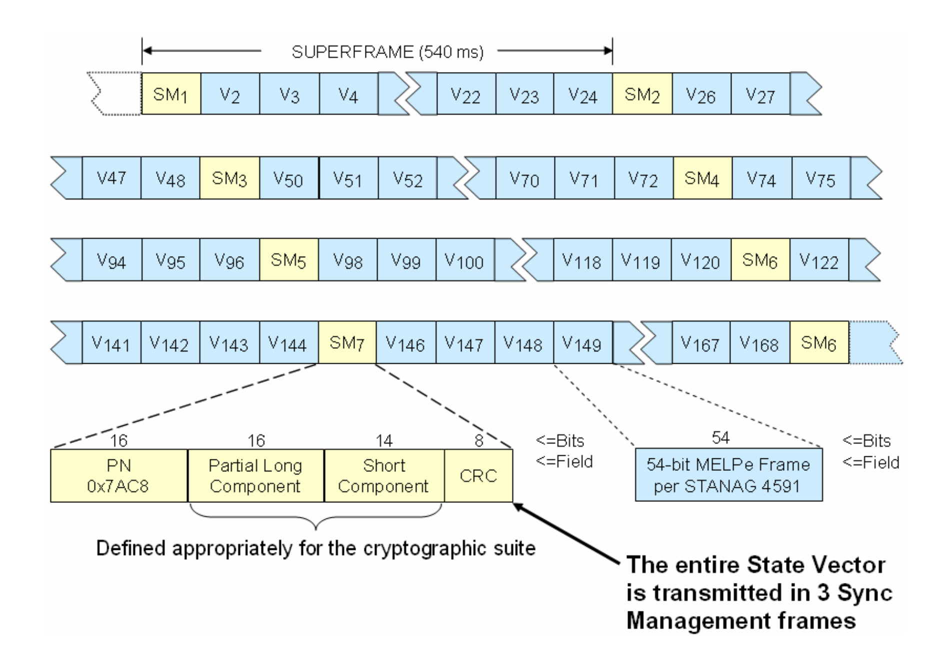


Figure 5.16 : *Secure 2400 bps MELP Voice – Blank and Burst – Format de transmission.*

5.6.2.3 - Secure MELP Voice – Burst without Blank

Le mode *Secure Burst without Blank* de MELP contient une trame *Sync Management* de 56 bits suivie de 24 trames de voix MELP. Les deux bits supplémentaires dans la trame *Sync Management* sont requis pour l'alignement des octets de la supertrame dû à la trame MELP. Dans ce cas-ci, la trame *Sync Management* ne remplace pas la première trame de voix MELP ; elle est insérée avant la première trame MELP. Ainsi, la supertrame est de 25 trames de long et aucune correction n'est nécessaire dans le récepteur. En insérant la trame *Sync Management* additionnelle dans la supertrame, le flux de bits résultant est à plus de 2400 bps.

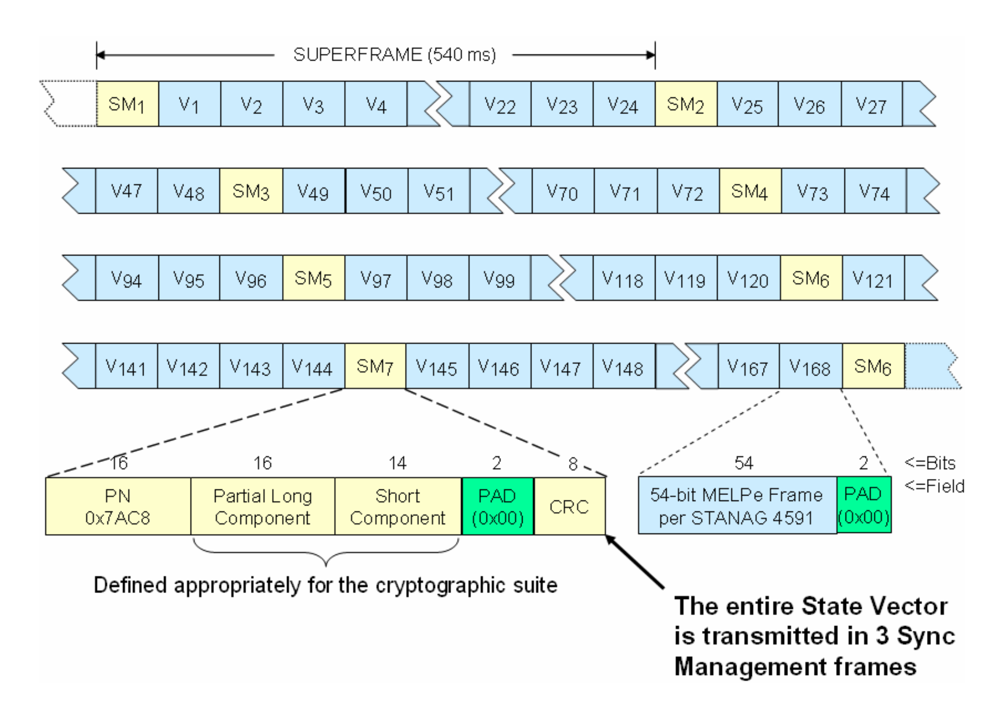


***Figure 5.17 :** Secure MELP Voice – Burst without Blank – Format de transmission.*

5.6.3 - Applications sécurisées de données

Deux applications sécurisées de données asynchrones sont spécifiées :

– *Secure Reliable Transport (RT) Asynchronous Data* ;
– *Secure 2400 bps Guaranteed Throughput (GT) Asynchronous Data.*

5.6.3.1 - Secure Reliable Transport Asynchronous Data

L'application *Secure RT Asynchronous Data* est l'application de données *MER* de FNBDT. Elle utilise les mêmes mécanismes de transport que ceux utilisés pour les messages d'établissement d'appel sécurisé pour la livraison des données d'utilisateur de façon fiable. La mise en trame, le *FEC* et la détection des erreurs résiduelles réduisent le débit maximal pour cette application à approximativement 70% du taux du canal, selon la longueur du message transmis.

Puisqu'un mécanisme de transport fiable est utilisé, toutes les données transmises arriveront au récepteur dans la plupart des conditions du canal. Il n'y a aucune occasion pour que le cryptosync soit perdu, et l'entrée en retard n'est pas une issue pour une application de transport fiable, qui par définition est point-à-point. Par conséquent, la maintenance de la synchronisation n'est pas exigée dans l'application *Secure RT Asynchronous Data*.

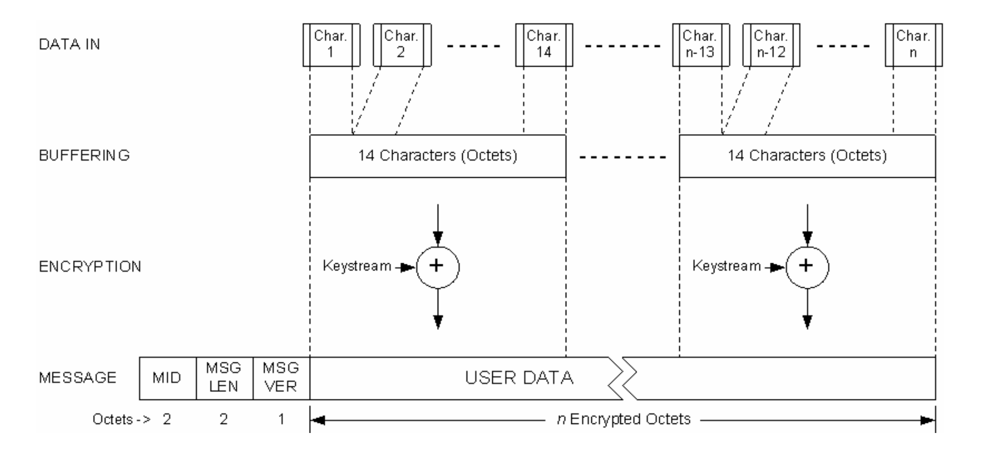


Figure 5.18 : *Préparation du message Secure RT Asynchronous Data.*

Une fois la transition à l'application *Secure RT Asynchronous Data* complétée, le terminal commence à accepter les caractères de données asynchrones plein texte (*plaintext*) au port de données de l'utilisateur. Les bits de début (*START*) et d'arrêt (*STOP*) seront enlevés avant le chiffrage et réinsérés au récepteur après déchiffrage. Les octets plein texte (caractères de données asynchrones sans les bits de début et d'arrêt) seront chiffrés et bufférisés jusqu'à ce qu'un nombre suffisant ait été rassemblé pour créer un message de données asynchrone RT sécurisé (*Secure RT Asynchronous Data*). Un message *Secure RT Asynchronous Data* peut contenir entre un octet de données utiles et 65532 (le maximum permis par les16 bits du champ *Message Length*).

Quand les bits de début et d'arrêt seront enlevés et jetés, les 8 bits de caractères de données de l'utilisateur seront alors formatés dans des blocs de 14-octet avant cryptage. S'il y a moins de 14 octets de texte chiffré à transmettre, un bourrage de bits à 0 peut être utilisé pour compléter un bloc à 14 octets.

5.6.3.2 - Secure 2400 bps Guaranteed Throughput Asynchronous Data

L'application *2400 bps GT Asynchronous Data* est une application facultative de données FNBDT. Elle utilise toute la capacité d'un canal à 2400 bps pour livrer des données utiles à 2400 bps sans dispositions de fiabilité. La signalisation pour le *Secure 2400 bps GT Asynchronous Data* doit être dans un format « *Burst without Blank* ». *Secure 2400 bps GT Asynchronous Data* doit être transmis dans des « supertrames » de 162 octets se composant d'une trame *Sync Management* de 64 bits suivies de 14 trames de données asynchrones de 11 octets chacune. La supertrame doit commencer par une trame *Sync Management* qui sera insérée, à intervalles périodiques, dans les données transmises. Il est à noter que des bits de début et d'arrêt pour les caractères de données asynchrones ne doivent pas être transmis et qu'aucune donnée d'utilisateur n'est jetée.

5.7 - Caractéristiques cryptographiques

Pour la sécurité, FNBDT utilise un bloc chiffrant (*block cipher*) fonctionnant en mode compteur (*counter mode*). Une nouvelle clé de chiffrage du trafic (*TEK*) est négociée pour chaque appel. Le *block cipher* est alimenté par un vecteur d'état (*SV – State Vector*) de 64 bits en entrée. Si la longueur du *block cipher* est plus longue que 64 bits, un remplisseur (*filler*) fixe est ajouté. La sortie du *block cipher* est ajoutée en *ou exclusif* (*xor*) aux trames de données MELP pour créer le texte chiffré (*cipher text*) qui est alors transmis.

Les deux bits de poids faible du vecteur d'état sont réservés pour des applications où la trame de données est plus longue que la sortie du *block cipher*. Les 42 bits suivants sont le compteur. Quatre bits sont utilisés pour représenter le mode de transmission. Ceci permet à plus d'un mode, par exemple voix et données, de fonctionner en même temps avec la même *TEK*. Les 16 bits de poids forts constituent l'identificateur de l'expéditeur. Ceci permet d'avoir plusieurs expéditeurs sur un seul canal, qui tous utiliseront la même *TEK*. Il est à noter que puisque le chiffrement global de FNBT est effectivement un flux chiffrant (*stream cipher*), il est essentiel que la même valeur du vecteur d'état ne soit jamais utilisée deux fois pour une *TEK* donnée. Aux débits des données MELP, un compteur de 42 bits permet un appel sur trois mille ans avant que le chiffrement ne se répète.

Pour la sécurité de *Type 1*, FNBDT utilise l'algorithme de cryptage *BATON*, un algorithme avec un bloc de 128 bits et une clé de 160 bits. Avec celui-ci ou d'autres codes de 128 bits, tels que *AES*, FNBDT spécifie que deux trames de données sont chiffrées avec chaque *cipher output bloc*, le premier commençant au bit 1, le second au bit 57 (c.-à-d. la prochaine frontière d'octet). Au moins une implémentation commerciale de qualité utilise le chiffrement *3DES* (*Triple Data Encryption Standard*).

CHAPITRE 6

ÉTUDE CRITIQUE DE FNBDT ET PERSPECTIVES

6.1 - Synthèse critique de FNBDT

Ce paragraphe expose une analyse critique de FNBDT portant sur des généralités, ainsi que sur l'impact du protocole sur les performances. D'un point de vue général, six points sont à signaler :

- FNBDT est un protocole complexe. En effet, il est définit sur plusieurs documents complémentaires ; celle du plan de signalisation faisant à elle seule plus de 260 pages !
- FNBDT est un protocole flexible puisqu'il prévoit dans la définition de son plan de signalisation, de l'espace protocolaire permettant une adaptation aux réseaux émergents et futurs ainsi que l'introduction de nouveaux types de données ;
- FNBDT assure la fiabilité du transport des données grâce à la trame *REPORT*, si on fonctionne en mode tramé, durant la phase de négociation des paramètres de sécurité. Or cette fiabilisation des données transmises est déjà assurée par la couche transport du modèle OSI au-dessus de laquelle se situe FNBDT. Donc, lorsque l'architecture FNBDT est combinée à une infrastructure de téléphonie sur IP, les trames *REPORT* seront redondantes ;
- FNBDT peut fonctionner avec une variété de vocodeurs, mais le standard requiert, au moins le support de MELP à 2400bps. Donc, FNDBT peut supporter des débits plus élevés. Par ailleurs, H.323 spécifie une série de codecs audio classés par débits allant de 5.3 à 64 kbps. Par conséquent, lorsque l'architecture FNBDT est combinée à H.323, il peut utiliser les codecs prévus pour H.323 ;
- pour l'établissement d'un appel FNBDT sécurisé, l'échange de quatre messages s'avère nécessaire, alors que l'échange d'un seul message suffit pour l'établissement d'un mode en clair ;
- l'établissement d'un appel FNBDT sécurisé commence par l'échange dans les messages *Capabilities* des modes opératoires mais aussi des clés correspondantes à ses modes. C'est une forme de *handshake* qui commence en clair et qui constitue donc un point faible de sécurité.

6.1.1 - *Les plus de FNBDT*

Qu'est-ce que FNBDT a introduit en plus ? Quatre points peuvent être mentionnés :

- FNBDT introduit une signalisation propre à lui qui renforce son indépendance par rapport aux couches de réseau sous-jacentes. Permettant ainsi une interopérabilité des réseaux à fils et ceux sans fils, il permet aussi une interopérabilité sécurisée entre équipements de tout genre ;
- FNBDT permet de sécuriser de bout-en-bout et la voix et les données, tout en offrant aussi la possibilité de transmettre la voix en clair ;
- le plan de signalisation de FNBDT distingue entre le mode de trafic tramé et le mode de trafic *full bandwidth* utilisé pour le transfert sécurisé de la voix. Il est donc innovant par le fait qu'il utilise toute la bande passante du canal pour transmettre la voix de façon sécurisée ;
- FNBDT prévoit un arrêt en douce des communications en cours sans éprouver le besoin de les avoir terminées. En effet, les trames *RESET* permettent une réinitialisation et une resynchronisation du système en cas de problèmes.

6.1.2 - *Impact de FNBDT sur les performances*

Quatre points principaux sont à mentionner quant à l'impact de FNBDT sur les performances :

- FNBDT présente une grande tolérance aux pertes de trames grâce aux acquittements positifs et réémissions sélectives identifiées par les trames *REPORT*,
- FNBDT présente aussi une grande tolérance aux déséquencements puisque côté récepteur, des mémoires permettent le stockage des trames déséquencées pour une livraison correcte,
- cependant, FNBDT présente une surcharge protocolaire (*overhead*) due à la taille fixe des trames. En effet, un message en mode tramé est délimité par 2 fanions de 8 octets chacun et peut être formé de 1 à 255 trames, chacune de 20 octets dont seuls 13 d'utiles, ce qui fait une surcharge protocolaire :
  - dans le cas d'une trame : on envoie 13 octets utiles sur (2*8 + 20), donc seuls 36% des octets envoyés sont utiles, ce qui fait une surcharge protocolaire de près de 64% ;
  - dans le cas de 255 trames : on envoie 255*13 octets utiles sur (2*8 + 255*20), donc 64,8% des octets envoyés sont utiles, ce qui réduit la charge protocolaire à près de 35% ;
- il faut noter qu'une fois la négociation des capacités terminée, FNBDT permet un passage en mode non tramé *full bandwidth*. Ceci permet un transfert de données de voix en provenance du vocodeur, directement chiffrées par la fonction de cryptage négociée ultérieurement durant la phase de négociation des capacités.

6.2 - Analyse comparative des mécanismes de sécurité

FNBDT ne garantit malheureusement pas tous les mécanismes de sécurité. C'est en effet, ce que j'explicite tout au long de ce paragraphe, dans le cadre d'une étude comparative entre les mécanismes de sécurité offerts par FNBDT et ceux offerts par SRTP (*Secure Real-time Transfer Protocol*, développé par le groupe de travail réseau de l'IETF), en me référant à H.235, le standard de sécurisation du trafic H.323, préparé par le groupe d'étude 16 de l'ITU-T.

Il est à noter que différents profils de sécurité sont proposés par H.235 comme exemples sur la façon de sécuriser le trafic H.323 : basé sur des clés symétriques, sur des signatures numériques, ou sur des infrastructures à clés publiques.

Il est aussi à noter qu'en plus de la protection du trafic de voix lui-même, H.235 assure une protection pour H.225 (établissement d'appel), H.245 (gestion de l'appel) et le *Gatekeeper Registration/Admission/Status* (RAS).

6.2.1 - Gestion des clés

Pour la gestion des clés, H.235 offre plusieurs possibilités dépendamment du profile utilisé : échange de clés Diffie-Hellman authentifiées et basées sur la cryptographie à clés publiques, attribution de mots de passe sur base de souscription, gestion de clés de session intégrées à H.235 ou allocation de certificats.

FNBDT, lui, utilise le système FIREFLY développé par la NSA.

Quant à SRTP, il gère deux types de clés : les clés maîtresses et les clés de sessions qui en dérivent et utilise pour cela des mécanismes de gestion de clés comme MIKEY, SDMS ou KEYMGT.

6.2.2 - Authentification

L'authentification avec H.235 est basée sur deux types de concepts : chiffrement symétrique ou partage de secret connu sous le nom de « souscription » avec trois variantes :

– basée sur un mot de passe avec chiffrement symétrique ;
– basée sur un mot de passe avec hachage (donc symétrique) – utilisation d'une fonction de hachage comme HMAC-SHA1-96 ;
– basée sur des certificats avec signatures (asymétrique – comme RSA) pour identifier l'utilisateur lui-même, pas seulement le point d'extrémité.

Comme troisième option, l'authentification avec H.235 peut être accomplie dans le contexte d'un protocole de sécurité séparé tel que TLS ou IPSec. L'authentification est ressortie pendant la connexion d'établissement d'appel sur le canal de signalisation. Un mode sécurisé de communication devrait être employé sur les canaux de signalisation (tels que TLS) avant l'échange des messages de connexion d'appel.

Avec FNBDT, l'authentification des utilisateurs est implicite à travers l'ensemble des messages échangés lors de l'établissement d'un appel sécurisé : échange des clés entre les deux utilisateurs, suivi d'une phase de spécification des paramètres cryptographiques et d'une phase de test de ces paramètres. Ce test permet de s'assurer que les deux utilisateurs utilisent bien l'algorithme de cryptage et les clés négociés entre les points d'extrémité.

Quant à SRTP, il assure uniquement l'authentification des messages qui est alors basée sur une fonction de hachage avec une clé invoquée pour authentifier l'en-tête et la charge utile des paquets RTP. Un MAC est apposé à la fin du paquet et vérifié par le récepteur qui le recalcule en utilisant le même processus par lequel il a été calculé. L'algorithme utilisé par défaut pour fournir l'authentification et l'intégrité est le HMAC-SHA1 avec une clé de 160 bits et un résultat de 80 bits. L'authentification de la source des messages est cependant uniquement assurée dans une communication de pair-à-pair, et pas dans une communication de groupe.

6.2.3 - Confidentialité

Avec H.235, la confidentialité est assurée par un chiffrement symétrique (DES à 56 bit, 3DES à 168 bits, RC-2 à 56-bit ou AES à 128 bits). Elle devrait être fournie pour le contrôle d'appel et les canaux de médias afin de protéger les données transportées sur ces canaux logiques. Pour fournir l'intimité des médias, un canal de contrôle privé, sur lequel établir le matériel de clé cryptographique et/ou installer les canaux logiques qui transporteront les flots de médias chiffrés, devrait être alloué. À cette fin, le canal entier de contrôle d'appel devrait être ouvert d'une façon sécurisée et négociée, protégeant ainsi la sélection d'algorithme cryptographique et les clés de chiffrage requises pour protéger des médias. Si le canal de contrôle doit fonctionner en mode non sécurisé, alors la clé cryptographique demandée pour chiffrer des canaux de médias devrait être transportée sur un canal logique H.235 spécifique.

Dans le programme de FNBDT, la sécurité est adressée par l'adoption du modèle de PKI/KMI pour l'échange des clés cryptographiques. Une spécification spécifique est dédiée à la définition de la couche cryptographique utilisée dans FNBDT, mais n'est pas publiée. Nous supposerons que le chiffrement des messages échangés est assuré en utilisant un algorithme cryptographique usuel (DES, 3DES, AES, etc.)

Pour assurer la confidentialité, SRTP utilise une approche de flot de clés pour chiffrer les flots d'information. La génération des flots de clés est accomplie par l'algorithme AES de chiffrement. SRTP met en application l'algorithme de chiffrage AES dans deux variantes différentes : AES en mode compteur entier segmenté (*Segmented Integer Counter Mode*) ou AES-f8 pour le cryptage des données UMTS. La transformation de chiffrement organise l'index et la clé secrète du paquet SRTP en un segment de flot de clés pseudo-aléatoires. Chaque segment de flot de clé chiffre un seul paquet SRTP. Le processus de chiffrement commencerait par une génération du segment du flot de clé correspondant au paquet, puis en faisant un ou-exclusif bit à bit de ce segment de flot de clé avec la charge utile du paquet de RTP pour produire la partie chiffrée des paquets SRTP.

6.2.4 - Intégrité

H.235 assure l'intégrité de l'information échangée au-dessus de tous les canaux logiques soit sur base de mots de passe, soit par l'utilisation de fonctions de hachage (HMAC-SHA1 ou MD5) déployées en même temps que les mécanismes d'authentification.

L'intégrité assurée avec FNBDT n'est pas cryptographique puisqu'elle se base uniquement sur le contrôle du CRC apposé à certains messages et non pas sur le résultat d'une fonction cryptographique. La vérification par CRC pourrait être considérée comme sorte de contrôle d'intégrité de l'information transportée dans les messages auxquels le CRC s'applique.

Avec SRTP, l'intégrité est déployée sur base d'une fonction de hachage, avec le mécanisme d'authentification. Cette intégrité utilise une fonction de hachage à sens unique (HMAC-SHA1), calculée sur tous les paquets SRTP et résultant en un digest (étiquette d'authentification). Ce digest sera apposé à la fin des paquets. L'intégrité est fournie aussi bien pour les communications point-à-point que pour des communications multicast et des sessions de groupe.

6.2.5 - Non rejeu

Des trois protocoles comparés (H.235, FNBDT et SRTP), seul SRTP assure une protection contre le rejeu et si l'intégrité est activée. Les en-têtes de RTP contiennent des numéros de séquence qui sont utilisés pour calculer les index des paquets et fournir cette protection contre les attaques par rejeu. Chaque récepteur SRTP maintient une liste de rejeu à lui seul qui indique les index de tous les paquets reçus et authentifiés en utilisant une technique de fenêtre coulissante, de sorte qu'une quantité fixe de stockage suffise pour la protection contre le rejeu. Après l'authentification d'un paquet, cette liste est mise à jour avec les nouveaux index.

Le non rejeu n'a pas été pris en considération et développé dans la recommandation H.235. Cependant, on pourrait trouver une solution en utilisant le numéro de séquence et les champs d'horodatage des en-têtes des paquets RTP échangés.

De même pour FNBDT, chaque message transporte une identification unique de la source (*Source ID*) des messages définis. Cette identification pourrait être utilisée pour établir une liste de rejeu soumise à un mécanisme de fenêtre coulissante, à vérifier par le récepteur afin de se protéger contre les attaques par rejeu.

6.2.6 - Non répudiation

Avec H.235, la non répudiation pourrait être fournie en utilisant la signature numérique en même temps qu'une fonction de hachage à sens unique telle que MD5 ou HMAC-SHA1. Dans sa dernière version, la recommandation H.235, garantit la non répudiation en se basant sur les PKI pour le profil correspondant.

FNBDT n'assure pas la non répudiation cryptographique.

De même, dans SRTP, la non répudiation n'est pas spécifiée ; elle pourrait être fournie par l'utilisation d'un certain algorithme tel que RSA.

6.3 - Étude comparative de FNBDT et SRTP

SRTP est un profil d'amélioration du standard RTP pour fournir la confidentialité, l'intégrité, l'authentification et la protection contre les attaques par rejeu. SRTP chiffre les données utiles tout en laissant l'en-tête du paquet en clair. SRTP est caractérisé par un débit élevé et une faible augmentation de la taille du paquet.

FNBDT et SRTP étant donc deux protocoles de sécurisation de bout-en-bout de la voix, indépendamment de la technologie du réseau sous-jacent, définissant ainsi un schéma d'interopérabilité sécurisée entre les systèmes à fils (« *wire* ») et sans fils (« *wireless* »), il serait intéressant de les comparer. Les deux protocoles présentent une grande tolérance aux pertes des paquets et à leur arrivée déséquencée, mais chacun à sa façon. Neuf différences principales ont été relevées :

i. FNBDT est le standard de communications sécurisées, proposé par la NSA en 1999 et récemment divulgué aux pays de l'OTAN qui sont alors susceptibles de l'adopter comme standard de sécurisation de la voix. Il a été défini en 4 documents principaux (cf. paragraphe 5.2), FNBDT 210 décrivant le plan de signalisation et étant le seul document publié.
   Quant à SRTP, il a été conçu par l'IETF qui l'a normalisé en mars 2004 par le RFC 3711 ;
ii. FNBDT correspond aux couches 5 et 6 du modèle OSI et se situe donc au-dessus de RTP, alors que SRTP se situe au-dessous de RTP et fait donc partie de la couche 4 du modèle OSI ;

iii. FNBDT permet de sécuriser la voix et les données tandis que SRTP ne sécurise pas les données. Tous deux offrent la possibilité de transmettre la voix en clair ;
iv. avec FNBDT, le choix du mode sécurisé nécessite pour toute opération l'échange d'une signalisation ; pour cela FNBDT requiert l'ouverture préalable d'un canal de données entre l'émetteur et le récepteur en mode natif (c.-à-d. non FNBDT).
    Par contre, SRTP ne nécessite ni l'échange de signalisation, ni l'ouverture préalable d'un canal ;
v. FNBDT distingue entre le mode tramé pour le transport de la signalisation à travers des messages ou groupes de trames et le mode *full bandwidth* où toute la bande du canal sous-jacent est utilisée pour la transmission de la voix sécurisée.
    Alors que dans SRTP, on n'a qu'un seul mode, le mode paquet ;
vi. en mode tramé de FNBDT, les messages sont délimités par 2 fanions de 8 octets et sont formés chacun de 1 à 255 trames de 20 octets chacune dont seuls 13 octets de charge utile ;
    Par contre, les paquets SRTP sont de taille variable, avec un en-tête minimal de 12 octets.
vii. FNBDT exige un débit minimal de 2400 bps, alors que SRTP n'impose aucune contrainte de débit, mais est caractérisé par un débit élevé ;
viii. FNBDT définit des messages de contrôle de sa couche *Transport* pour la fiabilisation et la synchronisation.
    Quant au protocole de l'IETF, c'est SRTCP qui sécurise RTCP, le protocole de contrôle de RTP et donc pas de protocole de contrôle de SRTP !
ix. dans FNBDT, un espace protocolaire est réservé à d'éventuelles extensions du protocole qui serait alors applicable aux nouvelles technologies émergentes, ainsi qu'à d'éventuels nouveaux types de données.
    Par contre, la flexibilité de SRTP réside uniquement dans la possibilité d'introduire de nouvelles transformations cryptographiques.

CHAPITRE 7

NOUVELLES PERSPECTIVES POUR LA SECURISATION DE LA TELEPHONIE

7.1 - Proposition d'intégration de FNBDT à H.323

Bien qu'il soit prévu pour être indépendant de l'infrastructure, FNBDT peut toutefois être intégré à H.323.

Un appel H.323 débute par une phase d'initialisation de l'appel pendant laquelle les messages de signalisation H.225.0 (Setup, Alerting, Connect, etc.) sont échangés entre les deux terminaux.

Le passage en mode FNBDT sera négocié dans des messages H.245. Nous définissons une nouvelle capacité de type **FNBDTSecurityCapability** qui permet aux entités des extrémités de négocier la sécurisation de l'appel de voix par les mécanismes de sécurité offerts par FNBDT. L'échange de messages FNBDT pour la sécurisation de l'appel de voix, comme le montre la figure 6.1, sera transporté sur un canal logique spécifique, ouvert par H.245 pour le mode FNBDT.

Nous ajouterons à la structure **Capability** l'entrée suivante :

```
Capability                        ::=CHOICE
{
  ...

  fnbdtSecurityCapability         FNBDTSecurityCapability

  ...
}
```

Durant la phase de négociation des paramètres FNBDT, ce dernier pourra utiliser les codecs de voix négociés préalablement par les deux entités aux extrémités dans des messages H.245 **Capapility**. Nous ajouterons à la structure **AudioCapability** le choix suivant du codec MELP à 2400 bps, assuré par FNBDT :

```
AudioCapability                   ::=CHOICE
{
  ...

  MELP2.4K                        INTEGER (1..256)
  ...

}
```

Notre proposition d'intégration de FNBDT à H.323 respecte bien les cinq phases principales requises pour l'établissement d'une conférence H.323 point-à-point (cf. paragraphe 3.5), c'est ce que montre d'ailleurs la figure 6.1 :

– phase A : initialisation de l'appel ;
– phase B : première communication et échange de capacités, dont la nouvelle capacité de type **FNBDTSecurityCapability** ;
– phase C : établissement de la communication audiovisuelle, avec les flots de média qui sont directement sécurisés par FNBDT à leur sortie du codeur ;
– phase D : dialogue, avec les flots de média, déjà sécurisés par FNBDT, qui sont encapsulés dans les paquets RTP ;
– phase E : fin.

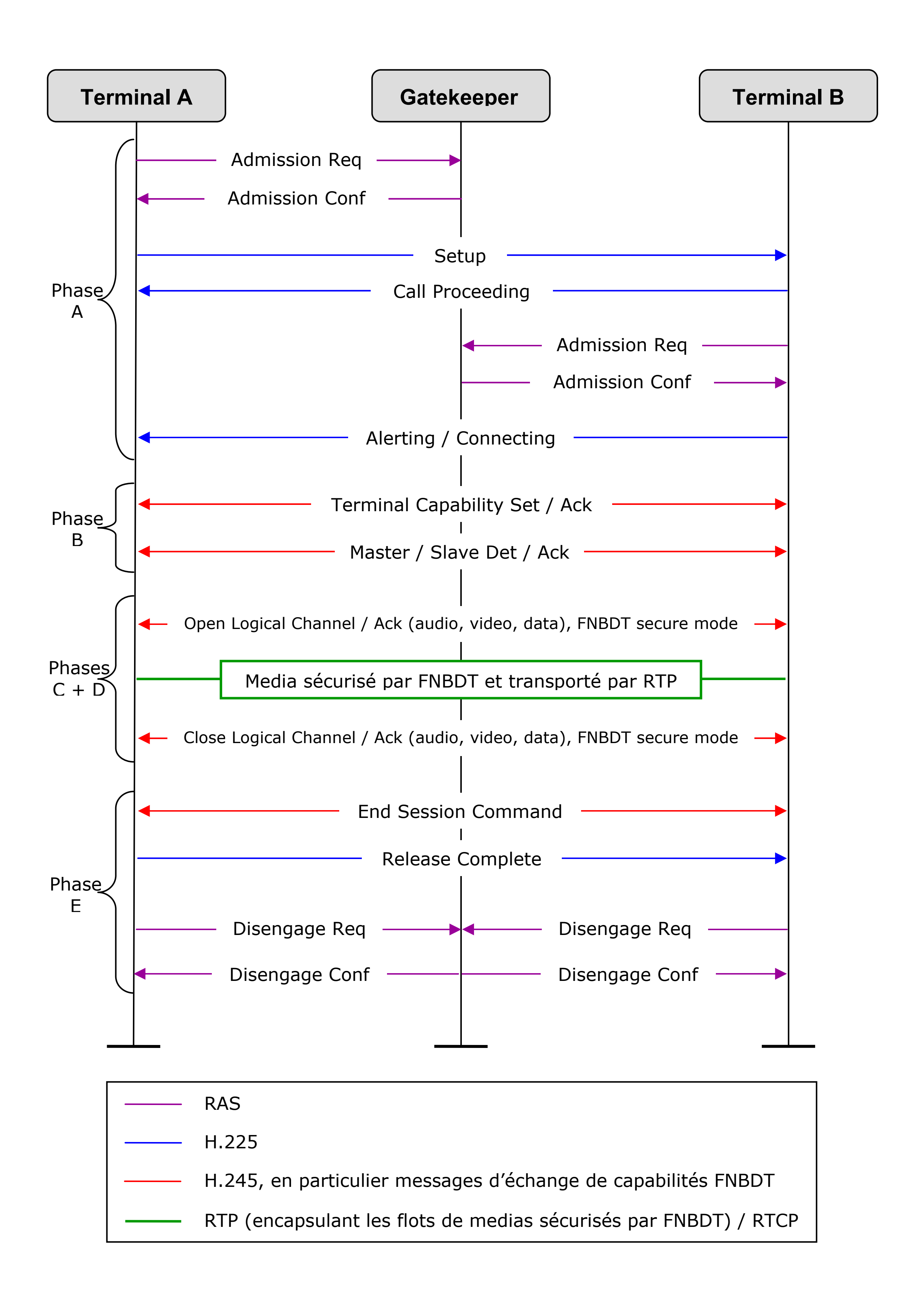


Figure 7.1 : *Intégration de FNBDT avec H.323.*

Afin de sécuriser l'échange des messages d'établissement d'appel et des messages de contrôle de flux médias, plusieurs solutions sont possibles, mais nous proposons dans notre solution d'intégration de FNBDT de se baser sur des sessions TCP sécurisées préalablement par TLS.

L'échange de messages de signalisation FNBDT, transportés par les messages de contrôle H.245 sur un canal TCP, sera donc sécurisé par TLS. Par contre, les messages transportant la voix, sortant directement du vocodeur, seront sécurisés par FNBDT et encapsulés dans des paquets RTP, qui sont transportés au-dessus de UDP.

7.2 - Motivations de la proposition

Comme solution de sécurisation de la voix, je propose donc d'intégrer FNBDT à H.323 en utilisant en plus TLS, et ce pour les raisons suivantes :

- H.323 est le protocole dominant pour les communications de voix et multimédia sur IP : la majorité des équipements de voix sur IP, des passerelles aux téléphones IP ou aux IP-PBX supportent actuellement le protocole H.323, et l'interopérabilité entre les constructeurs est maintenant excellente ;
- FNBDT est un protocole de sécurisation fiable des communications de bout-en-bout sur les réseaux *wire* et *wireless* ayant de nombreux points forts qui ont été surtout cités au paragraphe 6.1.1. Essentiellement, il permet l'interopérabilité sécurisée de communications de voix, vidéo et données indépendamment des couches protocolaires sous-jacentes, donc même si l'appel sort du réseau IP ;
- l'avantage de notre proposition réside dans la transmission séparée de la signalisation FNBDT et de l'information sécurisée, du moment où la première est transmise sur une connexion utilisant un port TCP, alors que la dernière l'est sur une connexion utilisant un port UDP ;
- le choix de TLS n'est pas aléatoire, puisqu'il est déjà défini par les recommandations de l'ITU-T comme pouvant être utilisé avec H.323 et puis, comme il ne peut pas fonctionner au-dessus de UDP, il permettra la sécurisation de la signalisation séparément de l'information utile, qui sera sécurisée par FNBDT (je rappelle que la voix dans ce cas utilise le mode *full bandwidth*). L'avantage de TLS par rapport à des protocoles comme IPSec ou ISAKMP réside donc dans l'inconvénient pour notre cas de ces derniers de fonctionner indépendamment du protocole de transport (TCP ou UDP) et qui sécuriserait deux fois l'information transmise au-dessus de UDP : une fois par FNBDT avant encapsulation dans RTP et une autre fois par IPSec ou ISAKMP ou autre protocole de sécurisation indépendamment du protocole de transport.

7.3 - Perspectives

La possibilité de sortir avec un nouveau protocole à partir des bons points de toutes les solutions possibles de sécurisation de la voix, n'est pas à exclure pour servir l'intérêt du sujet.

Il serait par exemple possible de penser à développer un nouveau protocole générique, de niveau applicatif dont le but est d'être déployé pour sécuriser un échange de communication de voix et essentiellement la voix sur IP et qui proposerait deux mécanismes nécessaires à la sécurité de la voix : l'authentification de l'utilisateur et la non répudiation de l'appel. Concernant les autres fonctions de sécurité, il serait alors possible dans une première approche de se référer au protocole SRTP pour assurer la confidentialité, l'intégrité et le non rejeu. Sachant que SRTP sécurise les paquets RTP, il peut être utilisé aussi bien avec H.323 qu'avec SIP.

CONCLUSION

Depuis les années quatre-vingt, les éditeurs de logiciels cherchent à utiliser le réseau informatique pour y véhiculer de la voix. En 1996, les premiers logiciels de téléphonie ou visioconférence sur IP ont vu le jour, de même que le standard H.323 normalisant le transfert de la voix sur les réseaux de données. Ces dernières années, la voix et la vidéo sur IP ont pris des dimensions de plus en plus importantes et les prévisions d'évolution du secteur sont optimistes avec des progrès sensibles déjà en 2008. Comme par ailleurs, la besoin de sécurité se fait ressentir de plus en plus fort par les temps qui courent et le cadre socio-économique ou nous vivons, la nécessité d'évoluer vers de nouvelles solutions IP sécurisantes de bout-en-bout et qui seraient universellement applicables se fait de plus en plus urgente, ce qui provoque aussi l'émergence de nouveaux standards.

Ce rapport a débuté par une présentation de la téléphonie sur IP, montrant que la condition sine qua non à sa sécurisation serait la sécurisation de la voix sur IP. Les points forts et ces points faibles de la téléphonie sur IP ont été présentés, suivis par les motivations techniques et économiques qui nous poussent à sécuriser la voix sur IP. Par la suite, les mécanismes de sécurité nécessaires à la sécurité de la voix sur IP ont été présentés. Spécifiquement les services de sécurité qui sont proposés avec le standard H.323 ; les requis de la sécurité de la voix sur IP ont été définis par la recommandation H.235 de l'ITU : IPsec assure des fonctions de sécurité par ses sous-protocoles, AH et ESP, et introduit une complexité au niveau de l'implémentation et du traitement, TLS est utilisé pour sécuriser les canaux de signalisation et de contrôle de H.323 et SRTP offre des services de sécurité pour les données de voix acheminées dans des paquets RTP. Bien que ces solutions permettent d'offrir une sécurité pour les appels de voix sur IP, elles restent cependant limitées au cadre d'un réseau IP. Si l'appel sort du réseau IP, cette sécurité n'est plus assurée par les solutions présentées. Un nouveau protocole de la NSA offre une sécurisation de la voix de bout-en-bout, indépendamment de l'infrastructure sous-jacente. Ce nouveau protocole a été présenté, analysé et comparé à SRTP : il constitue bien une solution de sécurisation de la voix, mais pas LA solution, et bien qu'il soit prévu pour être indépendant de l'infrastructure, il peut toutefois s'intégrer à H.323. C'est ce que j'ai proposé à la fin du dernier chapitre de ce mémoire, tout en explicitant les motivations qui m'ont poussé à ce choix.

La possibilité de sortir avec un nouveau protocole à partir des bons points de toutes les solutions possibles de sécurisation de la voix, n'est pas à exclure pour servir l'intérêt du sujet, mais sortirait du cadre de ce mémoire.

LISTE DES ABRÉVIATIONS

3DES	Triple Data Encryption Standard
ACELP	Algebraic CELP
ACF	Admission ConFirm
ADPCM	Adaptative Differential PCM
ADSL	Asymetrical Digital Subscriber Line
AEC	Acoustic Echo Cancellers
AES	Advanced Encryption Standard
AH	Authentication Header
ARQ[1]	Admission ReQuest
ARQ	Automatic Repeat reQuest
ATM	Asynchronous Transfer Mode
BCF	Bandwidth Change ConFirm
BCH	Bose-Chaudhuri, Hocquenghem (Error Correcting Code)
B-ISDN	BroadBand Integrated Services Digital Networks
bps	bits per second
BRQ	Bandwidth Change Request
CB	Citizen Band
CDMA	Code Division Multiple Access
CELP	Code Excited Linear Prediction
CKL	Compromised Key List
CNAME	Canonical Name
CODEC	COmpresseur/DÉCompresseur *ou* COdeur/DÉCodeur
COTS	Commercial-Off-The Shelf
CRC	Cyclic Redundancy Code
CS-ACELP	Conjugate Structure - Algebraic Code Excited Linear Prediction
CTI	Couplage Téléphonie / Informatique
DDVPC	Defense Digital Voice Processor Consortium
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DoD	Department of Defense
DoS	Denial of Service

[1] Au chapitre 3 seulement, dans le contexte de l'établissement d'appel H.323

E&M	Ear & Mouth (telephone signaling)
EEC	Electrical Echo Cancellers
EOM	End Of Message
ESP	Encapsulating Security Payload
FC	Frame Count
FCFS	First Come First Served
FEC	Forward Error Correction
FEC	Froward Error Correction
FNBDT	Future Narrow Band Digital Terminal
FS	Federal Standards
GRQ	Gatekeeper ReQuest
GSM EFR	GSM Enhanced Full Rate
GSM FR	GSM Full Rate
GSM HR	GSM Half Rate
GSM	Global System for Mobile communications
GT	Guaranteed Throughput
GW	Gateway
HMAC-SHA1	Hashed Message Authentication Code - Secure Hashing Algorithm 1
HTTP	HyperText Transfert Protocol
HTTPS	HTTP Secure *ou* HTTP over SSL
IAP	Internet Access Provider
ICO	Internet Connectivity Option
ICV	Integrity Check Value
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IOS	Internet Operating System
IP	Internet Protocol
IPBX	IP-PBX
IPSec	IP Security
IPv4	IP version 4
IPv6	IP version 6
ISAKMP	Internet Security Association and Key Management Protocol
ISP	Internet Service Provider
ISUP	Integrated Services User Part
ITU-T	International Telecommunication Union - Telecommunication standardization sector
IV	Initialization Vector
IWF	InterWorking Functions

KEYMGT	Key ManaGemenT Extensions (*for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP)*)
KMI	Key Management Infrastructure
LAN	Local Area Network
LD-CELP	Low Delay - CELP
MAC	Message Authentication Code
MC	Multipoint Controllers
MCU	Multipoint Control Unit
MD5	Message Digest 5
MEGACO	MEdia GAteway COntrol
MELP	Mixed Excitation Linear Prediction
MER	Minimal Essential Requirement
MGCP	Media Gateway to Media Controller Protocols
MIC	Modulation par Impulsions et Codage
MID	Message IDentification
MIKEY	Multimedia Internet KEYing
MOS	Mean Opinion Score
MP	Multipoint Processors
MP-MLQ	MultiPulse - Maximum Likelihood Quantization
NSA	National Security Agency
NSW	Non Secure Warning
OSI	Open Systems Interconnection
OTAN	Organisation du Traité de l'Atlantique Nord
PABX	Private Automatic Branch eXchange
PBX	Private Branch eXchange
PC	Personal Computer
PCM	Pulse Code Modulation
PGP	Pretty Good Privacy
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POTS	Plain Old Telephone Service
PSTN	Public Switched Telephone Network
QoS	Quality of Service
QSIG	Q-SIGnaling protocol

RAS	Registration, Admission, Status
RC-2	Ron's Code 2
RFC	Request For Comment
RNIS	Réseau Numérique à Intégration de Services
RSA	Rivest, Shamir, Adleman
RT	Reliable Transport
RTC	Réseau Téléphonique Commuté
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport Protocol
SA	Security Association
SCN	Switched Circuit Network
SDMS	Scientific Data Management System
SDNS	Secure Data Network System
SH	System High
SIP	Session Initialisation Protocol
SNA	System Network Architecture
SOM	Start Of Message
SRTCP	Secure RTCP
SRTP	Secure RTP
SSL	Secure Sockets Layer
SSRC	Synchronization SouRCe
STANAG	STANdardization AGreement
STE	Secure Terminal Equipment
STU	Secure Telephone Unit
SV	State Vector
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TDMA	Time Division Multiple Access
TE	Terminal Equipment
TEK	Traffic Encryption Key
TLS	Transport Layer Security
ToIP	Telephony over IP
TSAP	Transport Service Access Point
TTL	Time To Live
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
UN	UNclassified
USA	United States of America

VLAN	Virtual LAN
VoATM	Voice over ATM
VoFR	Voice over Frame Relay
VoIP	Voice over IP
VPN	Virtual Private Network
VPN/IP	VPN over IP
XML	eXtensible Markup Language

LISTE DES FIGURES

LISTE DES TABLEAUX

BIBLIOGRAPHIE

ALLIA (EL) Mourad. Développement d'un environnement de communication multimédia (voix et vidéo) sur Internet : mémoire **[en ligne]**. Maîtrise en génie électrique. Montréal : École de Technologie Supérieure, Université du Québec, 2002, 100 p. Disponible sur : <http://www.livia.etsmtl.ca/publications/2002/Memoie_Mourad.pdf> (consulté le 25-09-2004).

AMEZIANE Xavier, LEVEQUE Sébastien, ZEINER Lionel. Voice over Internet Protocol – projet réseaux : compte-rendu **[en ligne]**. Troisième année ESIAL. Nancy : Université Henri Poincaré – Nancy I, 2003, 39 p. Disponible sur : <http://www.loria.fr/~ichris/Teaching/ESIAL/ESIAL3/TPESR/VoIP.pdf> (consulté le 01-07-2004).

BAILLY F. La Voix sur IP **[en ligne]**. Disponible sur : <http://perso.club-internet.fr/f_bailly/VoIP/rapport_FINAL.htm> (consulté le 14-09-2004).

BASSIL Carole, BOULOS Nathalie, PUJOLLE Guy, et al. État de l'art de la sécurité de la voix. **In :** HEUDIASYC - Université de Technologie de Compiègne (UTC). SAR'04, 21-25 juin 2004, La Londe, Cote d'Azur, France.

BAUGHER M., MCGREW D., NASLUND M., et al. The Secure Real-time Transport Protocol (SRTP). IETF RFC 3711, mars 2004, 56 p.

BERGÉ Frédéric. Le protocole SIP brigue la téléphonie Internet. **[en ligne]**. Disponible sur : <http://www.01net.com/article/208827.html> (consulté le 21-09-2004).

BIGGS Maggie. Téléphonie sur IP : les 6 faiblesses qui rebutent les entreprises **[en ligne]**. Disponible sur : <http://www.zdnet.fr/techupdate/reseaux_telecoms/0,39020969,2097618,00.htm> (consulté le 22-09-2004).

BOGER Yuval. Fine-tuning Voice over Packet services **[en ligne]**. United Kingdom : RADCOM Ltd., 1999. Disponible sur : <http://www.universalfone.com/voip.zip> (consulté le 30-06-2004).

BOUARD Annabelle. Renforcer la sécurité de la téléphonie sur IP d'entreprise **[en ligne]**. Disponible sur : <http://www.01net.com/article/249598.html> (consulté le 14-09-2004).

BREGMAN Judith, FIEVET Cyril. La voix sur IP **[en ligne]**. Disponible sur : <http://www.fing.org/index.php?num=4283,2> (consulté le 22-09-2004).

BRIAN ADAMSON R., COLE Raymond Jr., MCBETH Michael S. Architecture for secure network voice. **In :** IEEE. Military Communications Conference Proceedings, 1999, Milcom. USA : IEEE, 1999, pp 1454-1457

CARMONA Gérard. Intégration et mise en oeuvre d'applications de téléphonie IP sur une architecture mixte IP et RNIS : thèse professionnelle. Mastère Conception et Architecture de Réseaux. Paris : ENST, 2002, 109 p.

CARRIÓN Inmaculada, LIU Jing. The Security Architecture of H.323. **In :** Tik-110.501 Seminar on Network Security, 2000. Helsinki : Helsinki University of Technology, 2000, 24 p.

CESMO CONSULTING. Livre Blanc – Téléphonie sur IP **[en ligne]**. Paris : France Télécom, 2004. Disponible sur : <http://www.francetelecom.com/fr/entreprises/grandes_entreprises/actualites/att00021168/LB_TOIP.pdf> (consulté le 29-06-2004).

CHUTET Marc. ToIP – Téléphonie sur IP **[en ligne]**. Disponible sur : <http://www.frameip.com/toip/> (consulté le 29-06-2004).

COLLURA J.S., VAN ENGELSHOVEN R.J. Secure end-to-end communication scenarios for NATO. Technical Note 980. La Haye : OTAN, 2003, 46 p.

CORNU Jean-Michel. La Voix sur IP : quelle architecture ? **[en ligne]**. Disponible sur : <http://www.fing.org/version_imprimable.php?NumContenu=4339> (consulté le 21-09-2004).

COUVE Philippe, RAILLARD Gilles. Échelon : les grandes oreilles américaines **[en ligne]**. Disponible sur : <http://cdcp.free.fr/dossiers/echelon/echelon.htm> (consulté le 22-10-2004).

DANIEL E. J., TEAGUE K. A. Performance of FNBDT and Low Rate Voice (MELP) Over Packet Networks. **In :** Proc. 35th Asilomar Conference on Signals, Systems, and Computers, 4-7 novembre 2001, Pacific Grove, Californie. USA : IEEE, pp 1568-1572.

DANIEL E.J., TEAGUE K.A., SLEEZER R., et al. The Future Narrowband Digital Terminal. **In :** MWSCAS 2002. The 2002 45th Midwest Symposium On Circuits and Systems Conference. USA : IEEE, pp II-589 - II-592.

DEBEAUPUIS Tristan. La téléphonie sur IP voix. **In :** JRES'97, 2 septembre 1997, La Rochelle **[en ligne]**. Paris : HSC, 1997, 11 p. Disponible sur : <http://www.hsc.fr/ressources/articles/telephonie/telephonie.pdf> (consulté le 14-09-2004).

DIERKS T., ALLEN C. The TLS Protocol – Version 1.0. IETF RFC 2246, janvier 1999, 80 p.

DIGITAL SERVICES INGÉNIERIE. La Téléphonie sur IP – TOIP – VOIP **[en ligne]**. Disponible sur : <http://www.dsi13.fr/articles_87.htm> (consulté le 22-09-2004).

DUBOURG Olivier. FNBDT (Future Narrow Band Digital Terminal). Mastère spécialisé Conception et Architecture de Réseaux : soutenance. Paris : ENST, 2003.

DUDET Michel, COLLET Patrice, HERSENT Olivier, et al. Téléphonie sur Internet : quelles perspectives ? **In :** Les services de l'Internet. **[en ligne]**. France : France Telecom R&D, 1998. (Actes des Forums France Télécom Recherche, Mémento N°11.) Disponible sur : <http://www.rd.francetelecom.com/fr/conseil/mento11/chap3.pdf> (consulté le 29-08-2004).

GENERAL DYNAMICS. FNBDT Signaling Plan. Revision 1.1 USA : GENERAL DYNAMICS, 1999, 266 p.

GERBER Cheryl. Converging on Network Security. Military Information Technology **[en ligne]**. 2004, vol. 8, n°1. Disponible sur : <http://www.military-information-technology.com/archive_article.cfm?DocID=384> (consulté le 20-08-2004).

GUILL.net. La voix sur IP : H323 et Signalisation **[en ligne]**. Disponible sur : <http://www.guill.net/index.php?cat=3&pro=29> (consulté le 27-08-2004).

IT ASSET MANAGEMENT. Analyse sectorielle de février 2004 - Que faut-il penser de la téléphonie sur IP ? **[en ligne]**. Paris : IT Asset Management, 2004. Disponible sur : <www.itasset.com/3-Technologies__marches/pdf/secto0204.pdf> (consulté le 29-06-2004).

IT.CAL. « Préparons la téléphonie sur IP ». 7 Février 2002, Paris **[en ligne]**. Courbevoie : IT.CAL, 2002. Disponible sur : <http://www.itcal.com/analyses/20020207.pdf> (consulté le 01-07-2004).

ITU-T. Call signalling protocols and media stream packetization for packet-based multimedia communication systems. H.225 version 5, juillet 2003, 188 p.

ITU-T. Packet-based multimedia communications systems. H.323 version 5, juillet 2003, 298 p.

ITU-T. Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals. H.235 version 3, août 2003, 130 p.

KENT S., ATKINSON R. IP Authentication Header. IETF RFC 2402, novembre 1998, 22 p.

KENT S., ATKINSON R. IP Encapsulating Security Payload (ESP). IETF RFC 2406, novembre 1998, 22 p.

KENT S., ATKINSON R. Security Architecture for the Internet Protocol. IETF RFC 2401, novembre 1998, 66 p.

LE TALLEC Yann. La voix sur IP **[en ligne]**. Disponible sur : <http://www.adae.gouv.fr/upload/documents/voix_sur_ip.rtf> (consulté le 30-06-2004).

LÉVY-ABÉGNOLI Thierry. Externaliser le PBX ? Un choix crédible avec les Centrex IP **[en ligne]**. Disponible sur : <http://www.zdnet.fr/techupdate/reseaux_telecoms/0,39020969,39171511,00.htm> (consulté le 21-09-2004).

LÉVY-ABÉGNOLI Thierry. Huit arguments qui plaident pour la téléphonie sur IP **[en ligne]**. Disponible sur : <http://www.zdnet.fr/techupdate/reseaux_telecoms/0,39020969,39138367,00.htm> (consulté le 21-09-2004).

LUCK Jay. Introduction to FNBDT Signaling, 2004.

MAHMOUDI Hafid. VoIP : la téléphonie sur IP enfin prête **[en ligne]**. Disponible sur : <http://www.01net.com/article/247192.html> (consulté le 14-09-2004).

MCGREW David A. Counter Mode Security: Analysis and Recommendations. USA : Cisco Systems, Inc., 2002, 8 p.

MILLMAN Rene. La téléphonie sur IP ouvre la porte aux pirates **[en ligne]**. Disponible sur : <http://www.vnunet.fr/actu/article.htm?numero=9457&date=2002-03-20> (consulté le 29-06-2004).

MONTHORIN Loïc, REYNAUD Stéphane. 4PABX-IP pour PME. Décision micro & réseaux **[en ligne]**. 2004, n°575, pp 24-29. Disponible sur : <http://www.01net.com/Pdf/DMR20040112057503l.pdf> (consulté le 30-06-2004).

NSA. Securing the wireless environment – A Strategy for Wireless Security and Wired/Wireless Secure Interoperability. USA : NSA, 2000, 34 p.

NSA. Security for Voice Over Internet Protocol (VoIP). Chapter 5. Section 4. **In :** IATF **[en ligne]**. Release 3.1. USA : NSA, 2002. Disponible sur : <http://www.iatf.net/framework_docs/version-3_1/docfile.cfm?chapter=ch05s4> (consulté le 20-08-2004).

OLF – GOUVERNEMENT DU QUÉBEC. Vocabulaire d'Internet – telephony over Internet Protocol **[en ligne]**. Disponible sur : <http://www.olf.gouv.qc.ca/ressources/bibliotheque/dictionnaires/Internet/fiches/8358638.html> (consulté le 30-06-2004).

OTAN. The Future Narrowband Digital Terminal (FNBDT) **[en ligne]**. 2000. Disponible sur : <http://nc3a.info/MDS/FNBDT/FNBDT_NATO_BriefV9.ppt> (consulté le 21-10-2004).

POLICEONE. General Dynamics Decision Systems High Assurance Solutions **[en ligne]**. Disponible sur : <http://www.policeone.com/police-products/communications/articles/70111/> (consulté le 20-08-2004).

REPETTI J. Différents scénarios de déploiement téléphonie sur IP (ToIP) dans les collectivités municipales **[en ligne]**. Saint-Clément-les-Places – France : Erasme. 2004. Disponible sur : <http://reseau.erasme.org/article.php3?id_article=196> (consulté le 01-07-2004).

REPETTI J. Introduction à la voix sur IP (VoIP) **[en ligne]**. Saint-Clément-les-Places – France : Erasme, 2004. Disponible sur : <http://reseau.erasme.org/article.php3?id_article=164> (consulté le 01-07-2004).

RFI. Échelon : mode d'emploi **[en ligne]**. Disponible sur : <http://cdcp.free.fr/dossiers/echelon/emploi.htm> (consulté le 22-10-2004).

RIVIÈRE Philippe. Le système Échelon. Le Monde diplomatique, janvier 2000, pp 40-42 **[en ligne]**. Disponible sur : <http://www.monde-diplomatique.fr/mav/46/RIVIERE/m1> (consulté le 22-10-2004).

SCHULZRINNE H., CASNER S., FREDERICK R., et al. RTP: A Transport Protocol for Real-Time Applications. IETF RFC 3550, juillet 2003, 104 p.

SERHROUCHNI Ahmed. Étude technique de la téléphonie fixe et mobile sur Internet. Paris : ENST, 2004, 109 p.

SLEEZER R., DANIEL E., RAYMOND J., et al. Counter Mode Encryption for FNBDT/MELP. **In :** MWSCAS 2002. The 2002 45th Midwest Symposium On Circuits and Systems Conference. USA : IEEE, pp III-692 – III-695.

THAYER R., DORASWAMY N., GLENN R. IP Security – Document Roadmap. IETF RFC 2411, novembre 1998, 11 p.

UNIVERSAL FONE. Universal Fone : La téléphonie dans sa dimension universelle **[en ligne]**. Disponible sur : <http://www.universalfone.com/voip1.php> (consulté le 30-06-2004).

WIKIPEDIA. FNBDT **[en ligne]**. Disponible sur : <http://en.wikipedia.org/wiki/FNBDT> (consulté le 21-10-2004).

WOLF Daniel G. « Cybersecurity – Getting it Right » **[en ligne]**. USA : NSA, 2003, 17 p. Disponible sur : <http://www.nsa.gov/ia/Wolf_SFR_22_July_2003.pdf> (consulté le 20-08-2004).

YOLIN Jean-Michel. Internet et Entreprise : mirages et opportunités ? Pour un plan d'action – Contribution à l'analyse de l'économie de l'Internet. 8ème Ed. **[en ligne]**. France : Ministère de l'Economie, des Finances et de l'Industrie – Ministère délégué à l'Industrie, 2004, pp 29-30. Disponible sur : <http://www.telecom.gouv.fr/documents/yolin/1215mirage2004.pdf> (consulté le 30-06-2004).